Qualys. Enterprise

Scan Results

August 21, 2018

Report Summary	
User Name:	REQUESTER INFO REMOVED
Login Name:	
Company:	
User Role:	
Address:	
City:	
State:	
Zip:	
Country:	United States of America
Created:	08/21/2018 at 12:41:11 (GMT-0500)
Launch Date:	08/21/2018 at 12:16:23 (GMT-0500)
Active Hosts:	1
Total Hosts:	1
Type:	On demand
Status:	Finished
Reference:	scan/1534871783.70985
External Scanners:	64.39.99.6 (Scanner 10.2.48-1, Vulnerability Signatures 2.4.402-2)
Authentication:	Unix/Cisco/Checkpoint Firewall authentication was successful for 1 host
Duration:	00:06:19
Title:	Ad Hoc - Area9 - External 20180821
Asset Groups:	-
IPs:	18.214.224.66
Excluded IPs:	-
Options Profile:	SAT Profile - QA/AUT

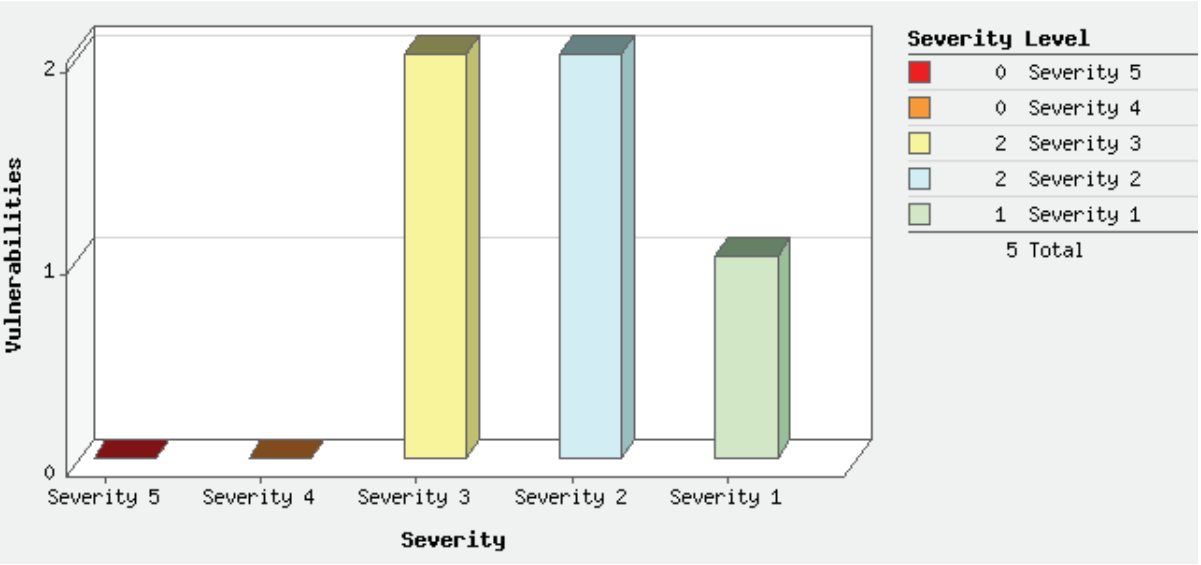
Summary of Vulnerabilities

Vulnerabilities Total	95	Security Risk (Avg)	3.0

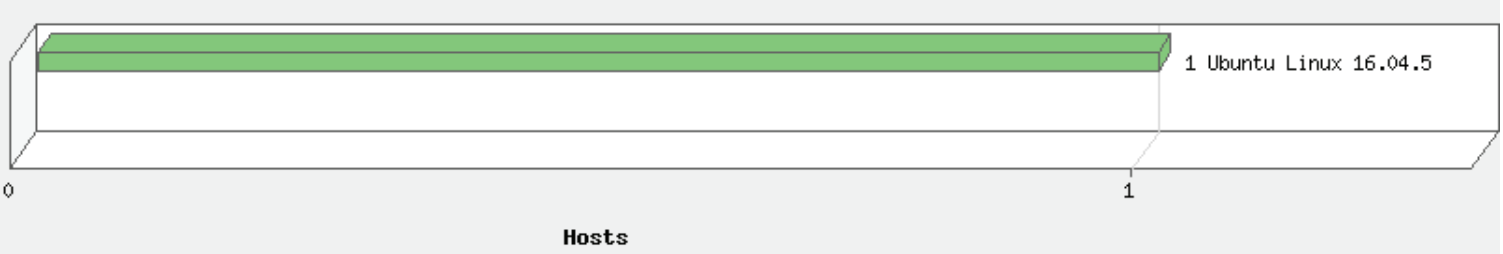
by Severity				
Severity	Confirmed	Potential	Information Gathered	Total
5	0	0	0	0
4	0	0	0	0
3	2	1	3	6
2	2	1	9	12
1	1	0	76	77
Total	5	2	88	95

5 Biggest Categories				
Category	Confirmed	Potential	Information Gathered	Total
Information gathering	0	0	25	25
Local	0	1	16	17
General remote services	2	1	14	17
Security Policy	0	0	13	13
Web server	0	0	9	9
Total	2	2	77	81

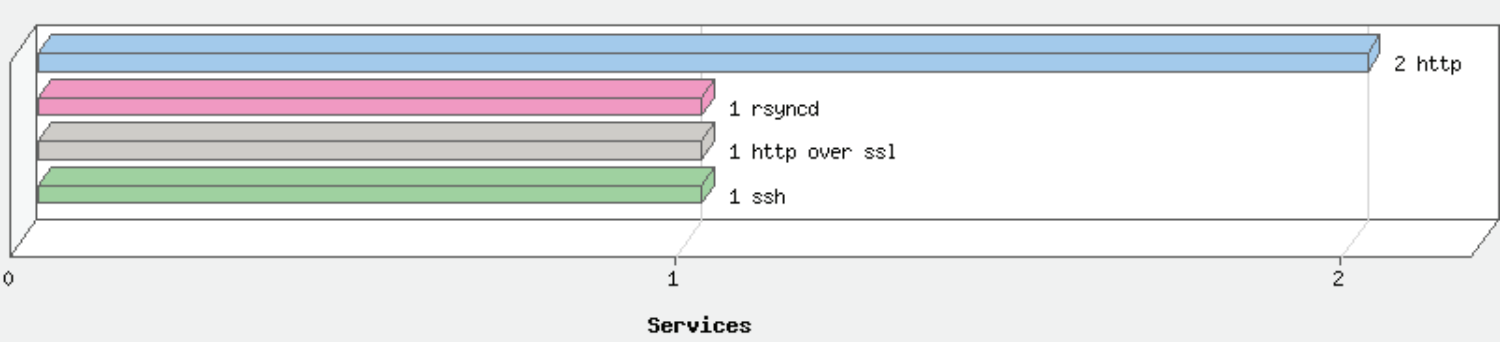
Vulnerabilities by Severity



Operating Systems Detected



Services Detected



Detailed Results

18.214.224.66 (ec2-18-214-224-66.compute-1.amazonaws.com, -) Ubuntu Linux 16.04.5
cpe:/o:canonical:ubuntu_linux:16.04.5:::

Vulnerabilities (5)

3 SSL/TLS Server supports TLSv1.0 port 443/tcp over SSL

QID:	38628	CVSS Base:	4.3 [1]
Category:	General remote services	CVSS Temporal:	3.9
CVE ID:	-		

Vendor Reference:	-			
Bugtraq ID:	-			
Service Modified:	01/18/2018	CVSS3 Base:	0	[1]
User Modified:	-	CVSS3 Temporal:	0	
Edited:	No			
PCI Vuln:	Yes			

THREAT:

TLS is capable of using a multitude of ciphers (algorithms) to create the public and private key pairs.
For example if TLSv1.0 uses either the RC4 stream cipher, or a block cipher in CBC mode.
RC4 is known to have biases and the block cipher in CBC mode is vulnerable to the POODLE attack.
TLSv1.0, if configured to use the same cipher suites as SSLv3, includes a means by which a TLS implementation can downgrade the connection to SSL v3.0, thus weakening security.
A POODLE-type (https://blog.qualys.com/ssllabs/2014/12/08/poodle-bites-tls) attack could also be launched directly at TLS without negotiating a downgrade.
This QID will be marked as a Fail for PCI as of May 1st, 2017 in accordance with the new standards. For existing implementations, Merchants will be able to submit a PCI False Positive / Exception Request and provide proof of their Risk Mitigation and Migration Plan, which will result in a pass for PCI up until June 30th, 2018.
Further details can be found at: NEW PCI DSS v3.2 and Migrating from SSL and Early TLS v1.1 (https://community.qualys.com/message/34120)

IMPACT:

An attacker can exploit cryptographic flaws to conduct man-in-the-middle type attacks or to decryption communications.
For example: An attacker could force a downgrade from the TLS protocol to the older SSLv3.0 protocol and exploit the POODLE vulnerability, read secure communications or maliciously modify messages.
A POODLE-type (https://blog.qualys.com/ssllabs/2014/12/08/poodle-bites-tls) attack could also be launched directly at TLS without negotiating a downgrade.

SOLUTION:

Disable the use of TLSv1.0 protocol in favor of a cryptographically stronger protocol such as TLSv1.2.
The following openssl commands can be used
to do a manual test:
openssl s_client -connect ip:port -tls1

If the test is successful, then the target support TLSv1

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

TLSv1.0 is supported

3 Birthday attacks against TLS ciphers with 64bit block size vulnerability (Sweet32) port 443/tcp over SSL

QID:	38657	CVSS Base:	5
Category:	General remote services	CVSS Temporal:	4.3
CVE ID:	CVE-2016-2183		
Vendor Reference:	-		
Bugtraq ID:	92630, 95568		
Service Modified:	05/30/2018	CVSS3 Base:	5.3
User Modified:	-	CVSS3 Temporal:	4.9
Edited:	No		
PCI Vuln:	No		

THREAT:
Legacy block ciphers having block size of 64 bits are vulnerable to a practical collision attack when used in CBC mode.
All versions of SSL/TLS
protocol support cipher suites which use DES, 3DES, IDEA or RC2 as the symmetric encryption cipher are affected.

IMPACT:
Remote attackers can obtain cleartext data via a birthday attack against a long-duration encrypted session.

SOLUTION:
Disable and stop using DES, 3DES, IDEA or RC2 ciphers.

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

CIPHER	KEY-EXCHANGE	AUTHENTICATION	MAC	ENCRYPTION(KEY-STRENGTH)	GRADE
TLSv1 WITH 64-BIT CBC CIPHERS IS SUPPORTED					
DES-CBC3-SHA	RSA	RSA	SHA1	3DES(168)	MEDIUM
EDH-RSA-DES-CBC3-SHA	DH	RSA	SHA1	3DES(168)	MEDIUM
ECDHE-RSA-DES-CBC3-SHA	ECDH	RSA	SHA1	3DES(168)	MEDIUM
TLSv1.1 WITH 64-BIT CBC CIPHERS IS SUPPORTED					
DES-CBC3-SHA	RSA	RSA	SHA1	3DES(168)	MEDIUM
EDH-RSA-DES-CBC3-SHA	DH	RSA	SHA1	3DES(168)	MEDIUM
ECDHE-RSA-DES-CBC3-SHA	ECDH	RSA	SHA1	3DES(168)	MEDIUM
TLSv1.2 WITH 64-BIT CBC CIPHERS IS SUPPORTED					
DES-CBC3-SHA	RSA	RSA	SHA1	3DES(168)	MEDIUM
EDH-RSA-DES-CBC3-SHA	DH	RSA	SHA1	3DES(168)	MEDIUM
ECDHE-RSA-DES-CBC3-SHA	ECDH	RSA	SHA1	3DES(168)	MEDIUM

2 HTTP Security Header Not Detected

port 8080/tcp

QID:	11827	CVSS Base:	4.3 [1]
Category:	CGI	CVSS Temporal:	3.5
CVE ID:	-		
Vendor Reference:	-		
Bugtraq ID:	-		
Service Modified:	08/07/2018	CVSS3 Base:	-
User Modified:	-	CVSS3 Temporal:	-
Edited:	No		
PCI Vuln:	Yes		

THREAT:
This QID reports the absence of the following HTTP headers (https://www.owasp.org/index.php/OWASP_Secure_Headers_Project#tab=Headers) according to CWE-693: Protection Mechanism Failure (https://cwe.mitre.org/data/definitions/693.html):
X-Frame-Options: This HTTP response header improves the protection of web applications against clickjacking attacks. Clickjacking, also known as a "UI redress attack", allows an attacker to use multiple transparent or opaque layers to trick a targeted user into clicking on a button or link on another page when they were intending to click on the the top level page.
X-XSS-Protection: This HTTP header enables the browser built-in Cross-Site Scripting (XSS) filter to prevent cross-site scripting attacks. X-XSS-Protection: 0; disables this functionality.
X-Content-Type-Options: This HTTP header prevents attacks based on MIME-type mismatch. The only possible value is nosniff. If your server returns X-Content-Type-Options: nosniff in the response, the browser will refuse to load the styles and scripts in case they have an incorrect MIME-type.
Content-Security-Policy: This HTTP header helps to detect and mitigate certain types of attacks, including Cross Site Scripting (XSS), packet sniffing

attacks and data injection attacks.
Strict-Transport-Security: The HTTP Strict-Transport-Security response header (HSTS) is a security feature that lets a web site tell browsers that it should only be communicated with using HTTPS, instead of using HTTP.
QID Detection Logic:
This unauthenticated QID looks for the presence of the following HTTP responses:
Valid directives for X-Frame-Options are:
X-Frame-Options: DENY - The page cannot be displayed in a frame, regardless of the site attempting to do so.
X-Frame-Options: SAMEORIGIN - The page can only be displayed in a frame on the same origin as the page itself.
X-Frame-Options: ALLOW-FROM RESOURCE-URL - The page can only be displayed in a frame on the specified origin.
Content-Security-Policy: frame-ancestors - This directive specifies valid parents that may embed a page using frame, iframe, object, embed, or applet
Valid directives for X-XSS-Protections are:
X-XSS-Protection: 1 - Enables XSS filtering (usually default in browsers). If a cross-site scripting attack is detected, the browser will sanitize the page (remove the unsafe parts).
X-XSS-Protection: 1; mode=block - Enables XSS filtering. Rather than sanitizing the page, the browser will prevent rendering of the page if an attack is detected.
X-XSS-Protection: 1; report=URI - Enables XSS filtering. If a cross-site scripting attack is detected, the browser will sanitize the page and report the violation. This uses the functionality of the CSP report-uri directive to send a report.
X-XSS-Protection: 0 disables this directive and hence is also treated as not detected.
A valid directive for X-Content-Type-Options: nosniff
A valid directive for Content-Security-Policy: <policy-directive>; <policy-directive>
A valid HSTS directive Strict-Transport-Security: max-age=<expire-time>; [; includeSubDomains][; preload]
NOTE: All report-only directives (where applicable) are considered invalid.

IMPACT:

Depending on the vulnerability being exploited, an unauthenticated remote attacker could conduct cross-site scripting, clickjacking or MIME-type sniffing attacks.

SOLUTION:

CWE-693: Protection Mechanism Failure mentions the following - The product does not use or incorrectly uses a protection mechanism that provides sufficient defense against directed attacks against the product. A "missing" protection mechanism occurs when the application does not define any mechanism against a certain class of attack. An "insufficient" protection mechanism might provide some defenses - for example, against the most common attacks - but it does not protect against everything that is intended. Finally, an "ignored" mechanism occurs when a mechanism is available and in active use within the product, but the developer has not applied it in some code path.
Customers are advised to set proper X-Frame-Options (https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Frame-Options), X-XSS-Protection (https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-XSS-Protection), Content Security Policy (https://developer.mozilla.org/en-US/docs/Web/HTTP/CSP), X-Content-Type-Options (https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Content-Type-Options) and Strict-Transport-Security (https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/Strict-Transport-Security) HTTP response headers.
Depending on their server software, customers can set directives in their site configuration or Web.config files. Few examples are:
X-Frame-Options:
Apache: Header always append X-Frame-Options SAMEORIGIN
nginx: add_header X-Frame-Options SAMEORIGIN;
HAProxy: rspadd X-Frame-Options:\ SAMEORIGIN
IIS: <HTTPPROTOCOL><CUSTOMHEADERS><ADD NAME="X-Frame-Options" VALUE="SAMEORIGIN"></ADD></CUSTOMHEADERS></HTTPPROTOCOL>
X-XSS-Protection:
Apache: Header always set X-XSS-Protection "1; mode=block"
PHP: header("X-XSS-Protection: 1; mode=block");
X-Content-Type-Options:
Apache: Header always set X-Content-Type-Options: nosniff
Content-Security-Policy: (Please note that these values may differ from website to website. The values below are for informational purposes only. The scanner simply looks for the presence of the security header.)
Apache: Header set Content-Security-Policy "script-src 'self'; object-src 'self'"
IIS: <SYSTEM.WEBSERVER><HTTPPROTOCOL><CUSTOMHEADERS><ADD NAME="Content-Security-Policy" VALUE="default-src 'self';"></ADD></CUSTOMHEADERS></HTTPPROTOCOL></SYSTEM.WEBSERVER>
nginx: add_header Content-Security-Policy "default-src 'self'; script-src 'self';
HTTP Strict-Transport-Security:
Apache: Header always set Strict-Transport-Security "max-age=31536000; includeSubDomains"
Nginx: add_header Strict-Transport-Security max-age=31536000;
Note: Network devices that include a HTTP/HTTPS console for administrative/management purposes often do not include all/some of the security headers. This is a known issue and it is recommend to contact the vendor for a solution.

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

X-Frame-Options or Content-Security-Policy: frame-ancestors HTTP Headers missing on port 8080.

GET / HTTP/1.1
Host: ec2-18-214-224-66.compute-1.amazonaws.com:8080
Connection: Keep-Alive

X-XSS-Protection HTTP Header missing on port 8080.
X-Content-Type-Options HTTP Header missing on port 8080.
Content-Security-Policy HTTP Header missing on port 8080.

2 HTTP Security Header Not Detected port 443/tcp

QID:	11827	CVSS Base:	4.3 [1]
Category:	CGI	CVSS Temporal:	3.5
CVE ID:	-		
Vendor Reference:	-		
Bugtraq ID:	-		
Service Modified:	08/07/2018	CVSS3 Base:	-
User Modified:	-	CVSS3 Temporal:	-
Edited:	No		
PCI Vuln:	Yes		

THREAT:
This QID reports the absence of the following HTTP headers (https://www.owasp.org/index.php/OWASP_Secure_Headers_Project#tab=Headers) according to CWE-693: Protection Mechanism Failure (https://cwe.mitre.org/data/definitions/693.html):
X-Frame-Options: This HTTP response header improves the protection of web applications against clickjacking attacks. Clickjacking, also known as a "UI redress attack", allows an attacker to use multiple transparent or opaque layers to trick a targeted user into clicking on a button or link on another page when they were intending to click on the the top level page.
X-XSS-Protection: This HTTP header enables the browser built-in Cross-Site Scripting (XSS) filter to prevent cross-site scripting attacks. X-XSS-Protection: 0; disables this functionality.
X-Content-Type-Options: This HTTP header prevents attacks based on MIME-type mismatch. The only possible value is nosniff. If your server returns X-Content-Type-Options: nosniff in the response, the browser will refuse to load the styles and scripts in case they have an incorrect MIME-type.
Content-Security-Policy: This HTTP header helps to detect and mitigate certain types of attacks, including Cross Site Scripting (XSS), packet sniffing attacks and data injection attacks.
Strict-Transport-Security: The HTTP Strict-Transport-Security response header (HSTS) is a security feature that lets a web site tell browsers that it should only be communicated with using HTTPS, instead of using HTTP.
QID Detection Logic:
This unauthenticated QID looks for the presence of the following HTTP responses:
Valid directives for X-Frame-Options are:
X-Frame-Options: DENY - The page cannot be displayed in a frame, regardless of the site attempting to do so.
X-Frame-Options: SAMEORIGIN - The page can only be displayed in a frame on the same origin as the page itself.
X-Frame-Options: ALLOW-FROM RESOURCE-URL - The page can only be displayed in a frame on the specified origin.
Content-Security-Policy: frame-ancestors - This directive specifies valid parents that may embed a page using frame, iframe, object, embed, or applet
Valid directives for X-XSS-Protections are:
X-XSS-Protection: 1 - Enables XSS filtering (usually default in browsers). If a cross-site scripting attack is detected, the browser will sanitize the page (remove the unsafe parts).
X-XSS-Protection: 1; mode=block - Enables XSS filtering. Rather than sanitizing the page, the browser will prevent rendering of the page if an attack is detected.
X-XSS-Protection: 1; report=URI - Enables XSS filtering. If a cross-site scripting attack is detected, the browser will sanitize the page and report the violation. This uses the functionality of the CSP report-uri directive to send a report.
X-XSS-Protection: 0 disables this directive and hence is also treated as not detected.
A valid directive for X-Content-Type-Options: nosniff
A valid directive for Content-Security-Policy: <policy-directive>; <policy-directive>
A valid HSTS directive Strict-Transport-Security: max-age=<expire-time>; [; includeSubDomains][; preload]
NOTE: All report-only directives (where applicable) are considered invalid.

IMPACT:
Depending on the vulnerability being exploited, an unauthenticated remote attacker could conduct cross-site scripting, clickjacking or MIME-type sniffing attacks.

SOLUTION:
CWE-693: Protection Mechanism Failure mentions the following - The product does not use or incorrectly uses a protection mechanism that provides sufficient defense against directed attacks against the product. A "missing" protection mechanism occurs when the application does not define any mechanism against a certain class of attack. An "insufficient" protection mechanism might provide some defenses - for example, against the most common attacks - but it does not protect against everything that is intended. Finally, an "ignored" mechanism occurs when a mechanism is available and in active use within the product, but the developer has not applied it in some code path.
Customers are advised to set proper X-Frame-Options (https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Frame-Options), X-XSS-

Protection (https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-XSS-Protection), Content Security Policy (https://developer.mozilla.org/en-US/docs/Web/HTTP/CSP), X-Content-Type-Options (https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Content-Type-Options) and Strict-Transport-Security (https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/Strict-Transport-Security) HTTP response headers. Depending on their server software, customers can set directives in their site configuration or Web.config files. Few examples are:
X-Frame-Options:
Apache: Header always append X-Frame-Options SAMEORIGIN
nginx: add_header X-Frame-Options SAMEORIGIN;
HAProxy: rspadd X-Frame-Options:\ SAMEORIGIN
IIS: <HTTPPROTOCOL><CUSTOMHEADERS><ADD NAME="X-Frame-Options" VALUE="SAMEORIGIN"></ADD></CUSTOMHEADERS></HTTPPROTOCOL>
X-XSS-Protection:
Apache: Header always set X-XSS-Protection "1; mode=block"
PHP: header("X-XSS-Protection: 1; mode=block");
X-Content-Type-Options:
Apache: Header always set X-Content-Type-Options: nosniff
Content-Security-Policy: (Please note that these values may differ from website to website. The values below are for informational purposes only. The scanner simply looks for the presence of the security header.)
Apache: Header set Content-Security-Policy "script-src 'self'; object-src 'self'"
IIS: <SYSTEM.WEBSERVER><HTTPPROTOCOL><CUSTOMHEADERS><ADD NAME="Content-Security-Policy" VALUE="default-src 'self';"></ADD></CUSTOMHEADERS></HTTPPROTOCOL></SYSTEM.WEBSERVER>
nginx: add_header Content-Security-Policy "default-src 'self'; script-src 'self';
HTTP Strict-Transport-Security:
Apache: Header always set Strict-Transport-Security "max-age=31536000; includeSubDomains"
Nginx: add_header Strict-Transport-Security max-age=31536000;
Note: Network devices that include a HTTP/HTTPS console for administrative/management purposes often do not include all/some of the security headers. This is a known issue and it is recommend to contact the vendor for a solution.

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

X-Frame-Options or Content-Security-Policy: frame-ancestors HTTP Headers missing on port 443.
GET / HTTP/1.1
Host: ec2-18-214-224-66.compute-1.amazonaws.com
Connection: Keep-Alive

X-XSS-Protection HTTP Header missing on port 443.
X-Content-Type-Options HTTP Header missing on port 443.
Content-Security-Policy HTTP Header missing on port 443.

1 ICMP Timestamp Request

QID:	82003	CVSS Base:	0
Category:	TCP/IP	CVSS Temporal:	0
CVE ID:	CVE-1999-0524		
Vendor Reference:	-		
Bugtraq ID:	-		
Service Modified:	04/28/2009	CVSS3 Base:	-
User Modified:	-	CVSS3 Temporal:	-
Edited:	No		
PCI Vuln:	No		

THREAT:

ICMP (Internet Control and Error Message Protocol) is a protocol encapsulated in IP packets. It's principal purpose is to provide a protocol layer able to inform gateways of the inter-connectivity and accessibility of other gateways or hosts. "ping" is a well-known program for determining if a host is up or down. It uses ICMP echo packets. ICMP timestamp packets are used to synchronize clocks between hosts.

IMPACT:

Unauthorized users can obtain information about your network by sending ICMP timestamp packets. For example, the internal systems clock should not be disclosed since some internal daemons use this value to calculate ID or sequence numbers (i.e., on SunOS servers).

SOLUTION:
You can filter ICMP messages of type "Timestamp" and "Timestamp Reply" at the firewall level. Some system administrators choose to filter most types of ICMP messages for various reasons. For example, they may want to protect their internal hosts from ICMP-based Denial Of Service attacks, such as the Ping of Death or Smurf attacks.
However, you should never filter ALL ICMP messages, as some of them ("Don't Fragment", "Destination Unreachable", "Source Quench", etc) are necessary for proper behavior of Operating System TCP/IP stacks.
It may be wiser to contact your network consultants for advice, since this issue impacts your overall network reliability and security.

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:
Timestamp of host (network byte ordering): 17:17:20 GMT

Potential Vulnerabilities (2)

3 OpenSSH Username Enumeration Vulnerability

QID:	38726	CVSS Base:	5 [1]
Category:	General remote services	CVSS Temporal:	4.3
CVE ID:	CVE-2018-15473		
Vendor Reference:	OpenBSDH OpenSSH		
Bugtraq ID:	-		
Service Modified:	08/20/2018	CVSS3 Base:	-
User Modified:	-	CVSS3 Temporal:	-
Edited:	No		
PCI Vuln:	Yes		

THREAT:
OpenSSH (OpenBSD Secure Shell) is a set of computer programs providing encrypted communication sessions over a computer network using the SSH protocol.
A username enumeration vulnerability exists in OpenSSH, that a remote attacker could leverage to enumerate valid users on a targeted system. The attacker could try to enumerate users by transmitting malicious packets. Due to the vulnerability, if a username does not exist, then the server sends a SSH2_MSG_USERAUTH_FAILURE message to the attacker. If the username exists, then the server sends a SSH2_MSG_SERVICE_ACCEPT before calling fatal() and closes the connection.
Affected Versions:
All current OpenSSH installations are affected by this vulnerability.
QID Detection Logic:
Authenticated: Vulnerable OpenSSH versions are detected by running ssh -V command.
Unauthenticated: Vulnerable OpenSSH versions are detected from the banner exposed.

IMPACT:
Successful exploitation allows an attacker to enumerate usernames on a targeted system.

SOLUTION:
N/A
Workaround:Customers are advised to contact vendors for updates pertaining to this vulnerability.
Until the vendor responds, customers are advised to allow remote OpenSSH access to authorized IP addresses only.

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
Qualys
Reference: CVE-0000-0000

Description: OpenSSH Username Enumeration
Link: http://seclists.org/oss-sec/2018/q3/125

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:
Vulnerable OpenSSH version detected:

OpenSSH_7.2p2 Ubuntu-4ubuntu2.4, OpenSSL 1.0.2g 1 Mar 2016

2 IP Forwarding Enabled

QID:	115284	CVSS Base:	7.5
Category:	Local	CVSS Temporal:	6.8
CVE ID:	CVE-1999-0511		
Vendor Reference:	-		
Bugtraq ID:	-		
Service Modified:	12/17/2009	CVSS3 Base:	-
User Modified:	-	CVSS3 Temporal:	-
Edited:	No		
PCI Vuln:	Yes		

THREAT:
If this machine is not a router or a firewall, then IP forwarding should not be activated.

IMPACT:
If this machine is not intended to be a router, then it may allow a malicious user to access your internal network.

SOLUTION:
Disable IP fowarding by following the appropriate instructions below:

On Windows 2000 and Windows NT, set the value of the following
registry key to zero: HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters\IPEnableRouter
On Linux, insert this line in
your startup script: "sysctl -w net.ipv4.ip_forward=0"
On Solaris, HP-UX B11.11 and B11.00, insert this line in your startup
script: "ndd -set /dev/ip ip_forwarding 0"
On Mac OS X, insert this line in your startup script: "sysctl -w
net.inet.ip.forwarding=0"

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

sysctl net.ipv4.ip_forward
net.ipv4.ip_forward = 1

Information Gathered (88)

3 Remote Access or Management Service Detected

QID:	42017
Category:	General remote services

CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	07/25/2018
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
A remote access or remote management service was detected. If such a service is accessible to malicious users it can be used to carry different type of attacks. Malicious users could try to brute force credentials or collect additional information on the service which could enable them in crafting further attacks.
The Results section includes information on the remote access service that was found on the target.
Services like Telnet, Rlogin, SSH, windows remote desktop, pcAnywhere, Citrix Management Console, Remote Admin (RAdmin), VNC, OPENVPN and ISAKMP are checked.

IMPACT:
Consequences vary by the type of attack.

SOLUTION:
Expose the remote access or remote management services only to the system administrators or intended users of the system.

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:
Service name: SSH on TCP port 22.

3 Unix Group List

QID:	105130
Category:	Security Policy
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	05/04/2018
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
All Unix groups found at the host are listed in the result section. The following fields are provided in the order shown.
1) The group name. Group names are fairly arbitrary but it is a good idea to choose group names that express some idea about the function of the group.

2) The group's encrypted password. Group passwords encouraged poor security practices, so most modern Unix systems don't support them.

3) The group's unique numeric ID (GID).

4) All users in the group.

IMPACT:
Users can get elevated privileges if they are added to Unix groups.

SOLUTION:

Check to be sure that the information provided adheres to your security policy.

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

root:x:0:
daemon:x:1:
bin:x:2:
sys:x:3:
adm:x:4:syslog,ubuntu
tty:x:5:
disk:x:6:
lp:x:7:
mail:x:8:
news:x:9:
uucp:x:10:
man:x:12:
proxy:x:13:
kmem:x:15:
dialout:x:20:ubuntu
fax:x:21:
voice:x:22:
cdrom:x:24:ubuntu
floppy:x:25:ubuntu
tape:x:26:
sudo:x:27:ubuntu
audio:x:29:ubuntu
dip:x:30:ubuntu
www-data:x:33:
backup:x:34:
operator:x:37:
list:x:38:
irc:x:39:
src:x:40:
gnats:x:41:
shadow:x:42:
utmp:x:43:
video:x:44:ubuntu
sasl:x:45:
plugdev:x:46:ubuntu
staff:x:50:
games:x:60:
users:x:100:
nogroup:x:65534:
systemd-journal:x:101:
systemd-timesync:x:102:
systemd-network:x:103:
systemd-resolve:x:104:
systemd-bus-proxy:x:105:
input:x:106:
crontab:x:107:
syslog:x:108:
netdev:x:109:ubuntu
lxd:x:110:ubuntu
messagebus:x:111:
uuidd:x:112:
ssh:x:113:
mlocate:x:114:
admin:x:115:
ubuntu:x:1000:
wheel:x:1001:matrix
matrix:x:1002:
docker:x:999:
svc-qlys:x:1003:

 3 User Home Directory With Non-Restrictive Permissions

QID:	105155
Category:	Security Policy
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	06/01/2016
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
The home directory of the users shown in the result section have non-restrictive permissions. Ideally all home directories should have the following permissions:
Owner: read, write, execute
Group: read, execute
Other: (No Permission)

IMPACT:
Unauthorised users can have read, write or execute access.

SOLUTION:
Change the directory permissions by issuing the following command:

chmod -R 750 (directory name)

COMPLIANCE:
Type: CobIT
Section: DS5.4
Description: User Account Management
Ensure that requesting, establishing, issuing, suspending, modifying and closing user accounts and related user privileges are addressed by user account management. An approval procedure outlining the data or system owner granting the access privileges should be included. These procedures should apply for all users, including administrators (privileged users), internal and external users, for normal and emergency cases. Rights and obligations relative to access to enterprise systems and information are contractually arranged for all types of users. Perform regular management review of all accounts and related privileges.

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

```
drwxr-xr-x 7 matrix   matrix   4096 Aug 20 14:41 matrix
drwxr-xr-x 4 svc-qlys svc-qlys 4096 Aug 21 14:50 svc-qlys
drwxr-xr-x 5 ubuntu   ubuntu   4096 Aug 21 16:43 ubuntu
```

 2 Operating System Detected

QID:	45017
Category:	Information gathering
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	08/21/2017
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
Several different techniques can be used to identify the operating system (OS) running on a host. A short description of these techniques is provided below. The specific technique used to identify the OS on this host is included in the RESULTS section of your report.

1) TCP/IP Fingerprint: The operating system of a host can be identified from a remote system using TCP/IP fingerprinting. All underlying operating system TCP/IP stacks have subtle differences that can be seen in their responses to specially-crafted TCP packets. According to the results of this "fingerprinting" technique, the OS version is among those listed below.
Note that if one or more of these subtle differences are modified by a firewall or a packet filtering device between the scanner and the host, the fingerprinting technique may fail. Consequently, the version of the OS may not be detected correctly. If the host is behind a proxy-type firewall, the version of the operating system detected may be that of the firewall instead of the host being scanned.
2) NetBIOS: Short for Network Basic Input Output System, an application programming interface (API) that augments the DOS BIOS by adding special functions for local-area networks (LANs). Almost all LANs for PCs are based on the NetBIOS. Some LAN manufacturers have even extended it, adding additional network capabilities. NetBIOS relies on a message format called Server Message Block (SMB).
3) PHP Info: PHP is a hypertext pre-processor, an open-source, server-side, HTML-embedded scripting language used to create dynamic Web pages. Under some configurations it is possible to call PHP functions like phpinfo() and obtain operating system information.
4) SNMP: The Simple Network Monitoring Protocol is used to monitor hosts, routers, and the networks to which they attach. The SNMP service maintains Management Information Base (MIB), a set of variables (database) that can be fetched by Managers. These include "MIB_II.system. sysDescr" for the operating system.

IMPACT:
Not applicable.

SOLUTION:
Not applicable.

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

Operating System	Technique	ID
Ubuntu Linux 16.04.5	Unix login	
Linux 2.6	TCP/IP Fingerprint	U6930:22
cpe:/o:canonical:ubuntu linux:16.04.5:::	CPE	


2 Unix Users With root UserID

QID:	105139
Category:	Security Policy
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	02/12/2017
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
The result section displays UNIX users with a root UserID, that is users with UID of 0.

IMPACT:
Root privileges on a UNIX host permits a user complete control of the host's operating system, configuration, and services. Restricted use of this privilege is advised. Check to be sure the results adhere to your security policy.

SOLUTION:
Remove users that should not have root UserID according to your security policy.

COMPLIANCE:
Type: CobIT
Section: DS5.4
Description: User Account Management
Ensure that requesting, establishing, issuing, suspending, modifying and closing user accounts and related user privileges are addressed by user

account management. An approval procedure outlining the data or system owner granting the access privileges should be included. These procedures should apply for all users, including administrators (privileged users), internal and external users, for normal and emergency cases. Rights and obligations relative to access to enterprise systems and information are contractually arranged for all types of users. Perform regular management review of all accounts and related privileges.

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:
root

2 Unix Users With root GroupID

QID:	105140
Category:	Security Policy
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	02/12/2017
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
The result section displays UNIX users with a root GroupID, that is users with GID of 0.

IMPACT:
Root privileges on a UNIX host permits a user complete control of the host's operating system, configuration, and services. Restricted use of this privilege is advised. Check to be sure the results adhere to your security policy.

SOLUTION:
Remove users that should not have root GroupID according to your security policy.

COMPLIANCE:
Type: CobIT
Section: DS5.4
Description: User Account Management
Ensure that requesting, establishing, issuing, suspending, modifying and closing user accounts and related user privileges are addressed by user account management. An approval procedure outlining the data or system owner granting the access privileges should be included. These procedures should apply for all users, including administrators (privileged users), internal and external users, for normal and emergency cases. Rights and obligations relative to access to enterprise systems and information are contractually arranged for all types of users. Perform regular management review of all accounts and related privileges.

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:
root

2 List of Home Directories Associated with UserIDs

QID:	105207
Category:	Security Policy
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-

Service Modified:	02/12/2017
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
All users should have a default home directory assigned. The UserID and home directory associated with the userid are as follows.

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:
root:/root
daemon:/usr/sbin
bin:/bin
sys:/dev
sync:/bin
games:/usr/games
man:/var/cache/man
lp:/var/spool/lpd
mail:/var/mail
news:/var/spool/news
uucp:/var/spool/uucp
proxy:/bin
www-data:/var/www
backup:/var/backups
list:/var/list
irc:/var/run/ircd
gnats:/var/lib/gnats
nobody:/nonexistent
systemd-timesync:/run/systemd
systemd-network:/run/systemd/netif
systemd-resolve:/run/systemd/resolve
systemd-bus-proxy:/run/systemd
syslog:/home/syslog
_apt:/nonexistent
lxd:/var/lib/lxd/
messagebus:/var/run/dbus
uuidd:/run/uuidd
dnsmasq:/var/lib/misc
sshd:/var/run/sshd
pollinate:/var/cache/pollinate
ubuntu:/home/ubuntu
matrix:/home/matrix
svc-qlys:/home/svc-qlys

2 List of Valid Shells

QID:	105213
Category:	Security Policy
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	02/08/2017

User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
/etc/shells is a text file which contains the full pathnames of valid login shells. This detection gets the contents of /etc/shells file. More information can be found by "man shells" or "man getusershell".

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:
/bin/sh
/bin/dash
/bin/bash
/bin/rbash
/usr/bin/tmux
/usr/bin/screen

2 root Should Be Specified in Block List for FTP Users

QID:	105328
Category:	Security Policy
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	06/08/2016
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
As best practice root user should be present in the list of users blocked for File Transfer Protocol (FTP) access. A configuration file contains this list of local user names that the ftpd server does not allow remote FTP clients to use. The general name and location of this file is:
On Linux, Solaris and Mac - "/etc/ftpusers"
On HP-UX - "/etc/ftpd/ftpusers" or "/etc/ftpd/ftpaccess"
Note: On HP-UX, root permission is required to access /etc/ftpd/ftpusers file.
This vulnerability check requires read permission on above mentioned configuration files. Without permission this detection may give false results.

IMPACT:
N/A

SOLUTION:
Add root entry in the corresponding configuration file.

COMPLIANCE:
Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:
File "/etc/ftpusers" not present or not accessible

2 Web Server HTTP Protocol Versions port 80/tcp

QID:	45266
Category:	Information gathering
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	04/24/2017
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
This QID lists supported HTTP protocol (HTTP 1.x or HTTP 2) from remote web server.

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:
Remote Web Server supports HTTP version 1.x on 80 port.GET / HTTP/1.1

2 Web Server HTTP Protocol Versions port 8080/tcp

QID:	45266
Category:	Information gathering
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	04/24/2017
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
This QID lists supported HTTP protocol (HTTP 1.x or HTTP 2) from remote web server.

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:
Remote Web Server supports HTTP version 1.x on 8080 port.GET / HTTP/1.1

2 Web Server HTTP Protocol Versions port 443/tcp

QID:	45266
Category:	Information gathering
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	04/24/2017
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
This QID lists supported HTTP protocol (HTTP 1.x or HTTP 2) from remote web server.

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:
Remote Web Server supports HTTP version 1.x on 443 port.GET / HTTP/1.1

1 DNS Host Name

QID:	6
Category:	Information gathering
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	01/04/2018
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
The fully qualified domain name of this host, if it was obtained from a DNS server, is displayed in the RESULT section.

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

IP address	Host name
18.214.224.66	ec2-18-214-224-66.compute-1.amazonaws.com

1 Target Network Information

QID:	45004
Category:	Information gathering
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	08/15/2013
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
The information shown in the Result section was returned by the network infrastructure responsible for routing traffic from our cloud platform to the target network (where the scanner appliance is located).
This information was returned from: 1) the WHOIS service, or 2) the infrastructure provided by the closest gateway server to our cloud platform. If your ISP is routing traffic, your ISP's gateway server returned this information.

IMPACT:
This information can be used by malicious users to gather more information about the network infrastructure that may help in launching attacks against it.

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:
The network handle is: AT-88-Z
Network description:

Amazon Technologies Inc.

1 Internet Service Provider

QID:	45005
Category:	Information gathering
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	09/27/2013
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
The information shown in the Result section was returned by the network infrastructure responsible for routing traffic from our cloud platform to the target network (where the scanner appliance is located).
This information was returned from: 1) the WHOIS service, or 2) the infrastructure provided by the closest gateway server to our cloud platform. If your ISP is routing traffic, your ISP's gateway server returned this information.

IMPACT:
This information can be used by malicious users to gather more information about the network infrastructure that may aid in launching further attacks against it.

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:
The ISP network handle is: EQUINIX-IX-DC
ISP Network description:
Equinix, Inc.

1 Traceroute

QID:	45006
Category:	Information gathering
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	05/09/2003
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
Traceroute describes the path in realtime from the scanner to the remote host being contacted. It reports the IP addresses of all the routers in between.

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

Hops	IP	Round Trip Time	Probe	Port
1	64.39.99.3	0.11ms	ICMP	
2	216.52.125.61	0.45ms	ICMP	
3	216.52.127.72	1.01ms	ICMP	
4	64.95.158.246	0.49ms	ICMP	
5	64.95.159.33	0.49ms	ICMP	
6	206.126.236.68	0.68ms	ICMP	
7	54.239.111.234	10.98ms	ICMP	
8	54.239.110.176	0.51ms	ICMP	
9	54.239.110.139	1.71ms	ICMP	
10	54.239.108.163	0.98ms	ICMP	
11	52.93.24.104	1.06ms	ICMP	
12	52.93.24.99	0.90ms	ICMP	
13	*.*.*.*	0.00ms	Other	80
14	*.*.*.*	0.00ms	Other	80
15	*.*.*.*	0.00ms	Other	80
16	*.*.*.*	0.00ms	Other	80
17	*.*.*.*	0.00ms	Other	80
18	18.214.224.66	1.06ms	ICMP	

1 Unix Server Information

QID:	45037
Category:	Information gathering
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	11/29/2004
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
The following information was found about the Unix server:

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

UName	Linux <anon>.area9learning.com 4.4.0-1065-aws #75-Ubuntu SMP Fri Aug 10 11:14:32 UTC 2018 x86 64 x86 64 x86 64 GNU/Linux
Operating system	Linux
Vendor	Debian
Ubuntu Release	Description: Ubuntu 16.04.5 LTS
Product	Ubuntu Linux
Version	16.04.5
CPU	x86 64

1 Host Scan Time

QID:	45038
Category:	Information gathering
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	03/18/2016
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
The Host Scan Time is the period of time it takes the scanning engine to perform the vulnerability assessment of a single target host. The Host Scan Time for this host is reported in the Result section below.
The Host Scan Time does not have a direct correlation to the Duration time as displayed in the Report Summary section of a scan results report. The Duration is the period of time it takes the service to perform a scan task. The Duration includes the time it takes the service to scan all hosts, which may involve parallel scanning. It also includes the time it takes for a scanner appliance to pick up the scan task and transfer the results back to the service's Secure Operating Center. Further, when a scan task is distributed across multiple scanners, the Duration includes the time it takes to perform parallel host scanning on all scanners.
For host running the Qualys Windows agent this QID reports the time taken by the agent to collect the host metadata used for the most recent assessment scan.

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:
Scan duration: 368 seconds

Start time: Tue, Aug 21 2018, 17:17:20 GMT

End time: Tue, Aug 21 2018, 17:23:28 GMT

1 Host Names Found

QID:	45039
Category:	Information gathering

CVE ID: -
Vendor Reference: -
Bugtraq ID: -
Service Modified: 02/14/2005
User Modified: -
Edited: No
PCI Vuln: No

THREAT:
The following host names were discovered for this computer using various methods such as DNS look up, NetBIOS query, and SQL server name query.

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

Host Name	Source
ec2-18-214-224-66.compute-1.amazonaws.com	FQDN
<anon>.area9learning.com	System-configured

1 Contents of /etc/issue File

QID: 45046
Category: Information gathering
CVE ID: -
Vendor Reference: -
Bugtraq ID: -
Service Modified: 05/04/2005
User Modified: -
Edited: No
PCI Vuln: No

THREAT:
The /etc/issue file contains the login banner.

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:
Ubuntu 16.04.5 LTS \n \l

1 Linux Kernel Version Running

QID:	45097
Category:	Information gathering
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	09/14/2016
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
The Linux kernel version running on the system at the time of the scan is listed in the result section. This QID currently supports:
Red Hat Linux
Oracle Enterprise Linux
Suse
Fedora
Debian
Ubuntu
CentOS
Amazon Linux
Amazon Linux Bare Metal

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:
Running Kernel Version is: 4.4.0-1065-aws

1 Contents of rsyslog.conf File

QID:	45121
Category:	Information gathering
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	01/10/2011
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
The rsyslog.conf file is the main configuration file for the rsyslogd which logs system messages on *nix systems. This file specifies rules for logging. ryslog.conf is backward compatible with sysklogd's syslog.conf file.

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:
```
#  /etc/rsyslog.conf Configuration file for rsyslog.
#
#   For more information see
#   /usr/share/doc/rsyslog-doc/html/rsyslog_conf.html
#
#  Default logging rules can be found in /etc/rsyslog.d/50-default.conf


#################
#### MODULES ####
#################

module(load="imuxsock") # provides support for local system logging
module(load="imklog")   # provides kernel logging support
#module(load="immark")  # provides --MARK-- message capability

# provides UDP syslog reception
#module(load="imudp")
#input(type="imudp" port="514")

# provides TCP syslog reception
#module(load="imtcp")
#input(type="imtcp" port="514")

# Enable non-kernel facility klog messages
$KLogPermitNonKernelFacility on

###########################
#### GLOBAL DIRECTIVES ####
###########################

#
# Use traditional timestamp format.
# To enable high precision timestamps, comment out the following line.
#
$ActionFileDefaultTemplate RSYSLOG_TraditionalFileFormat

# Filter duplicated messages
$RepeatedMsgReduction on

#
# Set the default permissions for all log files.
#
$FileOwner syslog
$FileGroup adm
$FileCreateMode 0640
$DirCreateMode 0755
$Umask 0022
$PrivDropToUser syslog
$PrivDropToGroup syslog
```

#
Where to place spool and state files
#
$WorkDirectory /var/spool/rsyslog

#
Include all config files in /etc/rsyslog.d/
#
$IncludeConfig /etc/rsyslog.d/*.conf

1 "daemon.notice" Entry Missing in rsyslog.conf file

QID:	45122
Category:	Information gathering
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	01/10/2011
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
The rsyslog.conf file specifies rules for logging. The file contains information used by the rsyslogd to forward a system message to appropriate log files and/or users. An entry of the form:
daemon.notice [Tab] <path to logfile>
ensures that all conditions involving daemons (such as ftpd) that are not error conditions are logged in the specified log file.
This entry was found to be missing from the rsyslog.conf file on the target.

IMPACT:
N/A

SOLUTION:
Ensure that the absence of the daemon.notice entry is in compliance with your organization's security policy.

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:
module(load="imuxsock") # provides support for local system logging
module(load="imklog")   # provides kernel logging support

$KLogPermitNonKernelFacility on

$ActionFileDefaultTemplate RSYSLOG_TraditionalFileFormat

$RepeatedMsgReduction on

$FileOwner syslog
$FileGroup adm
$FileCreateMode 0640
$DirCreateMode 0755
$Umask 0022
$PrivDropToUser syslog
$PrivDropToGroup syslog

$WorkDirectory /var/spool/rsyslog

$IncludeConfig /etc/rsyslog.d/*.conf

1 Python Installed on Host

QID:	45127
Category:	Information gathering
CVE ID:	-
Vendor Reference:	Python
Bugtraq ID:	-
Service Modified:	11/30/2016
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
Python is installed on target host. Python is a powerful dynamic programming language that is used in a wide variety of application domains. Python is available for all major operating systems including Windows, Linux/Unix, OS/2 etc.
Note: For Windows Systems
To get the exact version of Python installed on the target, look for the string followed by '#define PY_VERSION' in the result section. A target can have more than one version of Python installed.

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:
2.7.12 (default, Dec 4 2017, 14:50:18)
[GCC 5.4.0 20160609]

1 Installed Packages on Unix and Linux Operating Systems

QID:	45141
Category:	Information gathering
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	05/03/2015
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
This QID lists installed rpm packages or operating system vendor specific packages on the target Unix/Linux system.
Supported Unix or Linux Operating Systems:
RedHat Linux
CentOS
Suse
Fedora

Oracle Enterprise Linux
Debian
Ubuntu
IBM AIX
Solaris
Mac OS X
NOTE: If the system has more than 200 packages, this qid lists only first 200 packages.

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

accountsservice	0.6.40-2ubuntu11.3
acl	2.2.52-3
acpid	1:2.0.26-1ubuntu2
adduser	3.113+nmu3ubuntu4
apparmor	2.10.95-0ubuntu2.9
apport	2.20.1-0ubuntu2.18
apport-symptoms	0.20
apt	1.2.27
apt-transport-https	1.2.27
apt-utils	1.2.27
at	3.1.18-2ubuntu1
aufs-tools	1:3.2+20130722-1.1ubuntu1
base-files	9.4ubuntu4.7
base-passwd	3.5.39
bash	4.3-14ubuntu1.2
bash-completion	1:2.1-4.2ubuntu1.1
bcache-tools	1.0.8-2
bind9-host	1:9.10.3.dfsg.P4-8ubuntu1.10
binutils	2.26.1-1ubuntu1~16.04.6
bsdmainutils	9.0.6ubuntu3
bsdutils	1:2.27.1-6ubuntu3.6
btrfs-tools	4.4-1ubuntu1
build-essential	12.1ubuntu2
busybox-initramfs	1:1.22.0-15ubuntu1
busybox-static	1:1.22.0-15ubuntu1
byobu	5.106-0ubuntu1
bzip2	1.0.6-8
ca-certificates	20170717~16.04.1
certbot	0.26.1-1+ubuntu16.04.1+certbot+2
cgroupfs-mount	1.2
cloud-guest-utils	0.27-0ubuntu25.1
cloud-init	18.3-9-g2e62cb8a-0ubuntu1~16.04.2
cloud-initramfs-copymods	0.27ubuntu1.5
cloud-initramfs-dyn-netconf	0.27ubuntu1.5
command-not-found	0.3ubuntu16.04.2
command-not-found-data	0.3ubuntu16.04.2

console-setup	1.108ubuntu15.4
console-setup-linux	1.108ubuntu15.4
coreutils	8.25-2ubuntu3~16.04
cpio	2.11+dfsg-5ubuntu1
cpp	4:5.3.1-1ubuntu1
cpp-5	5.4.0-6ubuntu1~16.04.10
cron	3.0pl1-128ubuntu2
cryptsetup	2:1.6.6-5ubuntu2.1
cryptsetup-bin	2:1.6.6-5ubuntu2.1
curl	7.47.0-1ubuntu2.8
dash	0.5.8-2.1ubuntu2
dbus	1.10.6-1ubuntu3.3
dctrl-tools	2.24-2
debconf	1.5.58ubuntu1
debconf-i18n	1.5.58ubuntu1
debian-goodies	0.64
debianutils	4.7
dh-python	2.20151103ubuntu1.1
diffutils	1:3.3-3
distro-info-data	0.28ubuntu0.8
dmeventd	2:1.02.110-1ubuntu10
dmidecode	3.0-2ubuntu0.1
dmsetup	2:1.02.110-1ubuntu10
dns-root-data	2018013001~16.04.1
dnsmasq-base	2.75-1ubuntu0.16.04.5
dnsutils	1:9.10.3.dfsg.P4-8ubuntu1.10
docker-ce	18.06.0~ce~3-0~ubuntu
dosfstools	3.0.28-2ubuntu0.1
dpkg	1.18.4ubuntu1.4
dpkg-dev	1.18.4ubuntu1.4
e2fslibs:amd64	1.42.13-1ubuntu1
e2fsprogs	1.42.13-1ubuntu1
eatmydata	105-3
ed	1.10-2
eject	2.1.5+deb1+cvs20081104-13.1ubuntu0.16.04.1
ethtool	1:4.5-1
fakeroot	1.20.2-1ubuntu1
file	1:5.25-2ubuntu1.1
findutils	4.6.0+git+20160126-2
fontconfig-config	2.11.94-0ubuntu1.1
fonts-dejavu-core	2.35-1
fonts-ubuntu-font-family-console	1:0.83-0ubuntu2
friendly-recovery	0.2.31ubuntu1
ftp	0.17-33
fuse	2.9.4-1ubuntu3.1
g++	4:5.3.1-1ubuntu1
g++-5	5.4.0-6ubuntu1~16.04.10
gawk	1:4.1.3+dfsg-0.1
gcc	4:5.3.1-1ubuntu1
gcc-5	5.4.0-6ubuntu1~16.04.10
gcc-5-base:amd64	5.4.0-6ubuntu1~16.04.10
gcc-6-base:amd64	6.0.1-0ubuntu1
gdisk	1.0.1-1build1
geoip-database	20160408-1
gettext-base	0.19.7-2ubuntu3

gir1.2-glib-2.0:amd64	1.46.0-3ubuntu1
git	1:2.7.4-0ubuntu1.4
git-man	1:2.7.4-0ubuntu1.4
gnupg	1.4.20-1ubuntu3.3
gnupg-curl	1.4.20-1ubuntu3.3
gpgv	1.4.20-1ubuntu3.3
grep	2.25-1~16.04.1
groff-base	1.22.3-7
grub-common	2.02~beta2-36ubuntu3.18
grub-gfxpayload-lists	0.7
grub-legacy-ec2	18.3-9-g2e62cb8a-0ubuntu1~16.04.2
grub-pc	2.02~beta2-36ubuntu3.18
grub-pc-bin	2.02~beta2-36ubuntu3.18
grub2-common	2.02~beta2-36ubuntu3.18
gzip	1.6-4ubuntu1
hdparm	9.48+ds-1ubuntu0.1
hibagent	1.0.1-0ubuntu1~16.04.1
hostname	3.16ubuntu2
ifenslave	2.7ubuntu1
ifupdown	0.8.10ubuntu1.4
info	6.1.0.dfsg.1-5
init	1.29ubuntu4
init-system-helpers	1.29ubuntu4
initramfs-tools	0.122ubuntu8.11
initramfs-tools-bin	0.122ubuntu8.11
initramfs-tools-core	0.122ubuntu8.11
initscripts	2.88dsf-59.3ubuntu2
insserv	1.14.0-5ubuntu3
install-info	6.1.0.dfsg.1-5
iproute2	4.3.0-1ubuntu3.16.04.3
iptables	1.6.0-2ubuntu3
iputils-ping	3:20121221-5ubuntu2
iputils-tracepath	3:20121221-5ubuntu2
irqbalance	1.1.0-2ubuntu1
isc-dhcp-client	4.3.3-5ubuntu12.10
isc-dhcp-common	4.3.3-5ubuntu12.10
iso-codes	3.65-1
kbd	1.15.5-1ubuntu5
keyboard-configuration	1.108ubuntu15.4
klibc-utils	2.0.4-8ubuntu1.16.04.4
kmod	22-1ubuntu5
krb5-locales	1.13.2+dfsg-5ubuntu2
language-selector-common	0.165.4
less	481-2.1ubuntu0.2
libaccountsservice0:amd64	0.6.40-2ubuntu11.3
libacl1:amd64	2.2.52-3
libalgorithm-diff-perl	1.19.03-1
libalgorithm-diff-xs-perl	0.04-4build1
libalgorithm-merge-perl	0.08-3
libapparmor-perl	2.10.95-0ubuntu2.9
libapparmor1:amd64	2.10.95-0ubuntu2.9
libapt-inst2.0:amd64	1.2.27
libapt-pkg5.0:amd64	1.2.27
libasan2:amd64	5.4.0-6ubuntu1~16.04.10
libasn1-8-heimdal:amd64	1.7~git20150920+dfsg-4ubuntu1.16.04.1

libasprintf0v5:amd64	0.19.7-2ubuntu3
libatm1:amd64	1:2.5.1-1.5
libatomic1:amd64	5.4.0-6ubuntu1~16.04.10
libattr1:amd64	1:2.4.47-2
libaudit-common	1:2.4.5-1ubuntu2.1
libaudit1:amd64	1:2.4.5-1ubuntu2.1
libbind9-140:amd64	1:9.10.3.dfsg.P4-8ubuntu1.10
libblkid1:amd64	2.27.1-6ubuntu3.6
libbsd0:amd64	0.8.2-1
libbz2-1.0:amd64	1.0.6-8
libc-bin	2.23-0ubuntu10
libc-dev-bin	2.23-0ubuntu10
libc6:amd64	2.23-0ubuntu10
libc6-dev:amd64	2.23-0ubuntu10
libcap-ng0:amd64	0.7.7-1
libcap2:amd64	1:2.24-12
libcap2-bin	1:2.24-12
libcc1-0:amd64	5.4.0-6ubuntu1~16.04.10
libcilkrts5:amd64	5.4.0-6ubuntu1~16.04.10
libcomerr2:amd64	1.42.13-1ubuntu1
libcryptsetup4:amd64	2:1.6.6-5ubuntu2.1
libcurl3-gnutls:amd64	7.47.0-1ubuntu2.8
libdb5.3:amd64	5.3.28-11ubuntu0.1
libdbus-1-3:amd64	1.10.6-1ubuntu3.3
libdbus-glib-1-2:amd64	0.106-1
libdebconfclient0:amd64	0.198ubuntu1
libdevmapper-event1.02.1:amd64	2:1.02.110-1ubuntu10
libdevmapper1.02.1:amd64	2:1.02.110-1ubuntu10
libdns-export162	1:9.10.3.dfsg.P4-8ubuntu1.10
libdns162:amd64	1:9.10.3.dfsg.P4-8ubuntu1.10
libdpkg-perl	1.18.4ubuntu1.4
libdrm-common	2.4.91-2~16.04.1
libdrm2:amd64	2.4.91-2~16.04.1
libdumbnet1:amd64	1.12-7
libeatmydata1:amd64	105-3
libedit2:amd64	3.1-20150325-1ubuntu2
libelf1:amd64	0.165-3ubuntu1.1
liberror-perl	0.17-1.2
libestr0	0.1.10-1
libevent-2.0-5:amd64	2.0.21-stable-2ubuntu0.16.04.1
libexpat1:amd64	2.1.0-7ubuntu0.16.04.3
libexpat1-dev:amd64	2.1.0-7ubuntu0.16.04.3
libfakeroot:amd64	1.20.2-1ubuntu1
libfdisk1:amd64	2.27.1-6ubuntu3.6
libffi6:amd64	3.2.1-4
libfile-fcntllock-perl	0.22-3
libfontconfig1:amd64	2.11.94-0ubuntu1.1
libfreetype6:amd64	2.6.1-0.1ubuntu2.3
libfribidi0:amd64	0.19.7-1
libfuse2:amd64	2.9.4-1ubuntu3.1
libgcc-5-dev:amd64	5.4.0-6ubuntu1~16.04.10
libgcc1:amd64	1:6.0.1-0ubuntu1
libgcrypt20:amd64	1.6.5-2ubuntu0.5
libgd3:amd64	2.1.1-4ubuntu0.16.04.8
libgdbm3:amd64	1.8.3-13.1

libgeoip1:amd64	1.6.9-1
libgirepository-1.0-1:amd64	1.46.0-3ubuntu1
libglib2.0-0:amd64	2.48.2-0ubuntu4
libglib2.0-data	2.48.2-0ubuntu4
libgmp10:amd64	2:6.1.0+dfsg-2
libgnutls-openssl27:amd64	3.4.10-4ubuntu1.4
libgnutls30:amd64	3.4.10-4ubuntu1.4
libgomp1:amd64	5.4.0-6ubuntu1~16.04.10
libgpg-error0:amd64	1.21-2ubuntu1
libgpm2:amd64	1.20.4-6.1
libgssapi-krb5-2:amd64	1.13.2+dfsg-5ubuntu2
libgssapi3-heimdal:amd64	1.7~git20150920+dfsg-4ubuntu1.16.04.1
libhcrypto4-heimdal:amd64	1.7~git20150920+dfsg-4ubuntu1.16.04.1
libheimbase1-heimdal:amd64	1.7~git20150920+dfsg-4ubuntu1.16.04.1
libheimntlm0-heimdal:amd64	1.7~git20150920+dfsg-4ubuntu1.16.04.1
libhogweed4:amd64	3.2-1ubuntu0.16.04.1
libhx509-5-heimdal:amd64	1.7~git20150920+dfsg-4ubuntu1.16.04.1
libicu55:amd64	55.1-7ubuntu0.4
libidn11:amd64	1.32-3ubuntu1.2
libisc-export160	1:9.10.3.dfsg.P4-8ubuntu1.10
libisc160:amd64	1:9.10.3.dfsg.P4-8ubuntu1.10
libisccc140:amd64	1:9.10.3.dfsg.P4-8ubuntu1.10
libisccfg140:amd64	1:9.10.3.dfsg.P4-8ubuntu1.10
libisl15:amd64	0.16.1-1
libitm1:amd64	5.4.0-6ubuntu1~16.04.10
libjbig0:amd64	2.1-3.1
libjpeg-turbo8:amd64	1.4.2-0ubuntu3.1
libjpeg8:amd64	8c-2ubuntu8
libjson-c2:amd64	0.11-4ubuntu2
libk5crypto3:amd64	1.13.2+dfsg-5ubuntu2
libkeyutils1:amd64	1.5.9-8ubuntu1
libklibc	2.0.4-8ubuntu1.16.04.4
libkmod2:amd64	22-1ubuntu5
libkrb5-26-heimdal:amd64	1.7~git20150920+dfsg-4ubuntu1.16.04.1
libkrb5-3:amd64	1.13.2+dfsg-5ubuntu2
libkrb5support0:amd64	1.13.2+dfsg-5ubuntu2
libldap-2.4-2:amd64	2.4.42+dfsg-2ubuntu3.3
liblocale-gettext-perl	1.07-1build1
liblsan0:amd64	5.4.0-6ubuntu1~16.04.10
libltdl7:amd64	2.4.6-0.1
liblvm2app2.2:amd64	2.02.133-1ubuntu10
liblvm2cmd2.02:amd64	2.02.133-1ubuntu10
liblwres141:amd64	1:9.10.3.dfsg.P4-8ubuntu1.10
liblxc1	2.0.8-0ubuntu1~16.04.2
liblz4-1:amd64	0.0~r131-2ubuntu2
liblzma5:amd64	5.1.1alpha+20120614-2ubuntu2
liblzo2-2:amd64	2.08-1.2
libmagic1:amd64	1:5.25-2ubuntu1.1
libmnl0:amd64	1.0.3-5
libmount1:amd64	2.27.1-6ubuntu3.6
libmpc3:amd64	1.0.3-1
libmpdec2:amd64	2.4.2-1
libmpfr4:amd64	3.1.4-1
libmpx0:amd64	5.4.0-6ubuntu1~16.04.10
libmspack0:amd64	0.5-1ubuntu0.16.04.2

libncurses5:amd64	6.0+20160213-1ubuntu1
libncursesw5:amd64	6.0+20160213-1ubuntu1
libnetfilter-conntrack3:amd64	1.0.5-1
libnettle6:amd64	3.2-1ubuntu0.16.04.1
libnewt0.52:amd64	0.52.18-1ubuntu2
libnfnetlink0:amd64	1.0.1-3
libnih1:amd64	1.0.3-4.3ubuntu1
libnuma1:amd64	2.0.11-1ubuntu1.1
libp11-kit0:amd64	0.23.2-5~ubuntu16.04.1
libpam-modules:amd64	1.1.8-3.2ubuntu2.1
libpam-modules-bin	1.1.8-3.2ubuntu2.1
libpam-runtime	1.1.8-3.2ubuntu2.1
libpam-systemd:amd64	229-4ubuntu21.4
libpam0g:amd64	1.1.8-3.2ubuntu2.1
libparted2:amd64	3.2-15ubuntu0.1
libpcap0.8:amd64	1.7.4-2
libpci3:amd64	1:3.3.1-1.1ubuntu1.2
libpcre3:amd64	2:8.38-3.1
libperl5.22:amd64	5.22.1-9ubuntu0.5
libpipeline1:amd64	1.4.1-2
libplymouth4:amd64	0.9.2-3ubuntu13.5
libpng12-0:amd64	1.2.54-1ubuntu1.1
libpolkit-agent-1-0:amd64	0.105-14.1ubuntu0.1
libpolkit-backend-1-0:amd64	0.105-14.1ubuntu0.1
libpolkit-gobject-1-0:amd64	0.105-14.1ubuntu0.1
libpopt0:amd64	1.16-10
libprocps4:amd64	2:3.3.10-4ubuntu2.4
libpython-all-dev:amd64	2.7.12-1~16.04
libpython-dev:amd64	2.7.12-1~16.04
libpython-stdlib:amd64	2.7.12-1~16.04
libpython2.7:amd64	2.7.12-1ubuntu0~16.04.3
libpython2.7-dev:amd64	2.7.12-1ubuntu0~16.04.3
libpython2.7-minimal:amd64	2.7.12-1ubuntu0~16.04.3
libpython2.7-stdlib:amd64	2.7.12-1ubuntu0~16.04.3
libpython3-stdlib:amd64	3.5.1-3
libpython3.5:amd64	3.5.2-2ubuntu0~16.04.4
libpython3.5-minimal:amd64	3.5.2-2ubuntu0~16.04.4
libpython3.5-stdlib:amd64	3.5.2-2ubuntu0~16.04.4
libquadmath0:amd64	5.4.0-6ubuntu1~16.04.10
libreadline5:amd64	5.2+dfsg-3build1
libreadline6:amd64	6.3-8ubuntu2
libroken18-heimdal:amd64	1.7~git20150920+dfsg-4ubuntu1.16.04.1
librtmp1:amd64	2.4+20151223.gitfa8646d-1ubuntu0.1
libsasl2-2:amd64	2.1.26.dfsg1-14build1
libsasl2-modules:amd64	2.1.26.dfsg1-14build1
libsasl2-modules-db:amd64	2.1.26.dfsg1-14build1
libseccomp2:amd64	2.3.1-2.1ubuntu2~16.04.1
libselinux1:amd64	2.4-3build2
libsemanage-common	2.3-1build3
libsemanage1:amd64	2.3-1build3
libsepol1:amd64	2.4-2
libsigsegv2:amd64	2.10-4
libslang2:amd64	2.3.0-2ubuntu1.1
libsmartcols1:amd64	2.27.1-6ubuntu3.6
libsqlite3-0:amd64	3.11.0-1ubuntu1

libss2:amd64	1.42.13-1ubuntu1
libssl1.0.0:amd64	1.0.2g-1ubuntu4.13
libstdc++-5-dev:amd64	5.4.0-6ubuntu1~16.04.10
libstdc++6:amd64	5.4.0-6ubuntu1~16.04.10
libsystemd0:amd64	229-4ubuntu21.4
libtasn1-6:amd64	4.7-3ubuntu0.16.04.3
libtext-charwidth-perl	0.04-7build5
libtext-iconv-perl	1.7-5build4
libtext-wrapi18n-perl	0.06-7.1
libtiff5:amd64	4.0.6-1ubuntu0.4
libtinfo5:amd64	6.0+20160213-1ubuntu1
libtsan0:amd64	5.4.0-6ubuntu1~16.04.10
libubsan0:amd64	5.4.0-6ubuntu1~16.04.10
libudev1:amd64	229-4ubuntu21.4
libusb-0.1-4:amd64	2:0.1.12-28
libusb-1.0-0:amd64	2:1.0.20-1
libustr-1.0-1:amd64	1.0.4-5
libutempter0:amd64	1.1.6-3
libuuid1:amd64	2.27.1-6ubuntu3.6
libvpx3:amd64	1.5.0-2ubuntu1
libwind0-heimdal:amd64	1.7~git20150920+dfsg-4ubuntu1.16.04.1
libwrap0:amd64	7.6.q-25
libx11-6:amd64	2:1.6.3-1ubuntu2
libx11-data	2:1.6.3-1ubuntu2
libxau6:amd64	1:1.0.8-1
libxcb1:amd64	1.11.1-1ubuntu1
libxdmcp6:amd64	1:1.1.2-1.1
libxext6:amd64	2:1.3.3-1
libxml2:amd64	2.9.3+dfsg1-1ubuntu0.6
libxmlsec1	1.2.20-2ubuntu4
libxmlsec1-openssl	1.2.20-2ubuntu4
libxmuu1:amd64	2:1.1.2-2
libxpm4:amd64	1:3.5.11-1ubuntu0.16.04.1
libxslt1.1:amd64	1.1.28-2.1ubuntu0.1
libxtables11:amd64	1.6.0-2ubuntu3
libyaml-0-2:amd64	0.1.6-3
linux-aws	4.4.0.1065.67
linux-aws-headers-4.4.0-1061	4.4.0-1061.70
linux-aws-headers-4.4.0-1065	4.4.0-1065.75
linux-base	4.5ubuntu1~16.04.1
linux-headers-4.4.0-1061-aws	4.4.0-1061.70
linux-headers-4.4.0-1065-aws	4.4.0-1065.75
linux-headers-aws	4.4.0.1065.67
linux-image-4.4.0-1061-aws	4.4.0-1061.70
linux-image-4.4.0-1065-aws	4.4.0-1065.75
linux-image-aws	4.4.0.1065.67
linux-libc-dev:amd64	4.4.0-133.159
locales	2.23-0ubuntu10
login	1:4.2-3.1ubuntu5.3
logrotate	3.8.7-2ubuntu2.16.04.2
lsb-base	9.20160110ubuntu0.2
lsb-release	9.20160110ubuntu0.2
lshw	02.17-1.1ubuntu3.5
lsof	4.89+dfsg-0.1
ltrace	0.7.3-5.1ubuntu4

lvm2	2.02.133-1ubuntu10
lxc-common	2.0.8-0ubuntu1~16.04.2
lxcfs	2.0.8-0ubuntu1~16.04.2
lxd	2.0.11-0ubuntu1~16.04.4
lxd-client	2.0.11-0ubuntu1~16.04.4
make	4.1-6
makedev	2.3.1-93ubuntu2~ubuntu16.04.1
man-db	2.7.5-1
manpages	4.04-2
manpages-dev	4.04-2
mawk	1.3.3-17ubuntu2
mdadm	3.3-2ubuntu7.6
mime-support	3.59ubuntu1
mlocate	0.26-1ubuntu2
mount	2.27.1-6ubuntu3.6
mtr-tiny	0.86-1ubuntu0.1
multiarch-support	2.23-0ubuntu10
nano	2.5.3-2ubuntu2
ncurses-base	6.0+20160213-1ubuntu1
ncurses-bin	6.0+20160213-1ubuntu1
ncurses-term	6.0+20160213-1ubuntu1
net-tools	1.60-26ubuntu1
netbase	5.3
netcat-openbsd	1.105-7ubuntu1
nginx	1.10.3-0ubuntu0.16.04.2
nginx-common	1.10.3-0ubuntu0.16.04.2
nginx-core	1.10.3-0ubuntu0.16.04.2
ntfs-3g	1:2015.3.14AR.1-1ubuntu0.1
open-iscsi	2.0.873+git0.3b4b4500-14ubuntu3.5
open-vm-tools	2:10.2.0-3~ubuntu0.16.04.1
openssh-client	1:7.2p2-4ubuntu2.4
openssh-server	1:7.2p2-4ubuntu2.4
openssh-sftp-server	1:7.2p2-4ubuntu2.4
openssl	1.0.2g-1ubuntu4.13
os-prober	1.70ubuntu3.3
overlayroot	0.27ubuntu1.5
parted	3.2-15ubuntu0.1
passwd	1:4.2-3.1ubuntu5.3
pastebinit	1.5-1
patch	2.7.5-1ubuntu0.16.04.1
pciutils	1:3.3.1-1.1ubuntu1.2
perl	5.22.1-9ubuntu0.5
perl-base	5.22.1-9ubuntu0.5
perl-modules-5.22	5.22.1-9ubuntu0.5
pigz	2.3.1-2
plymouth	0.9.2-3ubuntu13.5
plymouth-theme-ubuntu-text	0.9.2-3ubuntu13.5
policykit-1	0.105-14.1ubuntu0.1
pollinate	4.33-0ubuntu1~16.04.1
popularity-contest	1.64ubuntu2
powermgmt-base	1.31+nmu1
procps	2:3.3.10-4ubuntu2.4
psmisc	22.21-2.1build1
python	2.7.12-1~16.04
python-all	2.7.12-1~16.04

python-all-dev	2.7.12-1~16.04
python-apt	1.1.0~beta1ubuntu0.16.04.2
python-apt-common	1.1.0~beta1ubuntu0.16.04.2
python-certbot-nginx	0.25.0-2+ubuntu16.04.1+certbot+1
python-dev	2.7.12-1~16.04
python-minimal	2.7.12-1~16.04
python-pip	8.1.1-2ubuntu0.4
python-pip-whl	8.1.1-2ubuntu0.4
python-pkg-resources	33.1.1-1+certbot~xenial+1
python-setuptools	33.1.1-1+certbot~xenial+1
python-wheel	0.29.0-1
python2.7	2.7.12-1ubuntu0~16.04.3
python2.7-dev	2.7.12-1ubuntu0~16.04.3
python2.7-minimal	2.7.12-1ubuntu0~16.04.3
python3	3.5.1-3
python3-acme	0.26.0-1+ubuntu16.04.1+certbot+1
python3-apport	2.20.1-0ubuntu2.18
python3-apt	1.1.0~beta1ubuntu0.16.04.2
python3-asn1crypto	0.22.0-2+ubuntu16.04.1+certbot+1
python3-blinker	1.3.dfsg2-1build1
python3-certbot	0.26.1-1+ubuntu16.04.1+certbot+2
python3-certbot-nginx	0.25.0-2+ubuntu16.04.1+certbot+1
python3-certifi	2017.4.17-2+ubuntu16.04.1+certbot+1
python3-cffi-backend	1.10.0-0.1+ubuntu16.04.1+certbot+1
python3-chardet	3.0.4-1+ubuntu16.04.1+certbot+2
python3-commandnotfound	0.3ubuntu16.04.2
python3-configargparse	0.11.0-1+certbot~xenial+1
python3-configobj	5.0.6-2+ubuntu16.04.1+certbot+1
python3-cryptography	1.9-1+ubuntu16.04.1+certbot+2
python3-dbus	1.2.0-3
python3-debian	0.1.27ubuntu2
python3-distupgrade	1:16.04.25
python3-funcsigs	0.4-2
python3-future	0.15.2-4+ubuntu16.04.1+certbot+3
python3-gdbm:amd64	3.5.1-1
python3-gi	3.20.0-0ubuntu1
python3-icu	1.9.2-2build1
python3-idna	2.5-1+ubuntu16.04.1+certbot+1
python3-jinja2	2.8-1
python3-josepy	1.0.1-1+ubuntu16.04.1+certbot+7
python3-json-pointer	1.9-3
python3-jsonpatch	1.19-3
python3-jwt	1.3.0-1ubuntu0.1
python3-markupsafe	0.23-2build2
python3-minimal	3.5.1-3
python3-mock	1.3.0-2.1ubuntu1
python3-newt	0.52.18-1ubuntu2
python3-oauthlib	1.0.3-1
python3-openssl	17.3.0-1~0+ubuntu16.04.1+certbot+1
python3-parsedatetime	2.4-3+ubuntu16.04.1+certbot+3
python3-pbr	1.8.0-4ubuntu1
python3-pkg-resources	33.1.1-1+certbot~xenial+1
python3-prettytable	0.7.2-3
python3-problem-report	2.20.1-0ubuntu2.18
python3-pyasn1	0.1.9-2+certbot~xenial+1

python3-pycurl	7.43.0-1ubuntu1
python3-pyparsing	2.0.3+dfsg1-1ubuntu0.1
python3-requests	2.18.1-1+ubuntu16.04.1+certbot+1
python3-requests-toolbelt	0.8.0-1+ubuntu16.04.1+certbot+1
python3-rfc3339	1.0-4+certbot~xenial+1
python3-serial	3.0.1-1
python3-six	1.11.0-1+ubuntu16.04.1+certbot+1
python3-software-properties	0.96.20.7
python3-systemd	231-2build1
python3-tz	2014.10~dfsg1-0ubuntu2
python3-update-manager	1:16.04.13
python3-urllib3	1.21.1-1+ubuntu16.04.1+certbot+1
python3-yaml	3.11-3build1
python3-zope.component	4.3.0-1+ubuntu16.04.1+certbot+3
python3-zope.event	4.2.0-1
python3-zope.hookable	4.0.4-4+ubuntu16.04.1+certbot+1
python3-zope.interface	4.3.2-1+ubuntu16.04.1+certbot+1
python3.5	3.5.2-2ubuntu0~16.04.4
python3.5-minimal	3.5.2-2ubuntu0~16.04.4
readline-common	6.3-8ubuntu2
rename	0.20-4
resolvconf	1.78ubuntu6
rsync	3.1.1-3ubuntu1.2
rsyslog	8.16.0-1ubuntu3
run-one	1.17-0ubuntu1
screen	4.3.1-2build1
sed	4.2.2-7
sensible-utils	0.0.9ubuntu0.16.04.1
sgml-base	1.26+nmu4ubuntu1
shared-mime-info	1.5-2ubuntu0.2
snapd	2.34.2
software-properties-common	0.96.20.7
sosreport	3.5-1~ubuntu16.04.3
squashfs-tools	1:4.3-3ubuntu2.16.04.3
ssh-import-id	5.5-0ubuntu1
strace	4.11-1ubuntu3
sudo	1.8.16-0ubuntu1.5
systemd	229-4ubuntu21.4
systemd-sysv	229-4ubuntu21.4
sysv-rc	2.88dsf-59.3ubuntu2
sysvinit-utils	2.88dsf-59.3ubuntu2
tar	1.28-2.1ubuntu0.1
tcpd	7.6.q-25
tcpdump	4.9.2-0ubuntu0.16.04.1
telnet	0.17-40
time	1.7-25.1
tmux	2.1-3build1
tzdata	2017c-0ubuntu0.16.04
ubuntu-cloudimage-keyring	2013.11.11
ubuntu-core-launcher	2.34.2
ubuntu-keyring	2012.05.19
ubuntu-minimal	1.361.1
ubuntu-release-upgrader-core	1:16.04.25
ubuntu-server	1.361.1
ubuntu-standard	1.361.1

ucf	3.0036
udev	229-4ubuntu21.4
ufw	0.35-0ubuntu2
uidmap	1:4.2-3.1ubuntu5.3
unattended-upgrades	0.90ubuntu0.9
update-manager-core	1:16.04.13
update-notifier-common	3.168.9
ureadahead	0.100.0-19
usbutils	1:007-4
util-linux	2.27.1-6ubuntu3.6
uuid-runtime	2.27.1-6ubuntu3.6
vim	2:7.4.1689-3ubuntu1.2
vim-common	2:7.4.1689-3ubuntu1.2
vim-runtime	2:7.4.1689-3ubuntu1.2
vim-tiny	2:7.4.1689-3ubuntu1.2
vlan	1.9-3.2ubuntu1.16.04.5
wget	1.17.1-1ubuntu1.4
whiptail	0.52.18-1ubuntu2
xauth	1:1.0.9-1ubuntu2
xdg-user-dirs	0.15-2ubuntu6.16.04.1
xfsprogs	4.3.0+nmu1ubuntu1.1
xkb-data	2.16-1ubuntu1
xml-core	0.13+nmu2
xz-utils	5.1.1alpha+20120614-2ubuntu2
zerofree	1.0.3-1
zlib1g:amd64	1:1.2.8.dfsg-2ubuntu4.1

 1 Netstat - Unix Connections

QID:	45191
Category:	Information gathering
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	10/09/2016
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
TCP/UDP connections detected on UNIX host.
Open ports disclose services available on the host.

IMPACT:
N/A

SOLUTION:
Disable unnecessary running services to reduce potential attack surface.

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

Local Address	Local Port	Remote Address	Remote Port	Connection Status
172.31.4.140	80	64.39.99.6	60469	TIME_WAIT
172.31.4.140	22	64.39.99.6	44798	ESTABLISHED
127.0.0.1	39506	127.0.0.1	8080	TIME_WAIT
172.31.4.140	443	64.39.99.6	53225	TIME_WAIT
172.31.4.140	443	64.39.99.6	53391	TIME_WAIT
172.31.4.140	443	64.39.99.6	53390	TIME_WAIT
172.31.4.140	22	217.71.227.251	35326	ESTABLISHED
127.0.0.1	39548	127.0.0.1	8080	TIME_WAIT
172.31.4.140	80	64.39.99.6	60429	TIME_WAIT
172.31.4.140	443	64.39.99.6	53217	TIME_WAIT
172.31.4.140	443	64.39.99.6	53357	TIME_WAIT
172.31.4.140	443	64.39.99.6	53220	TIME_WAIT
172.31.4.140	443	64.39.99.6	53335	TIME_WAIT
172.31.4.140	443	64.39.99.6	53392	TIME_WAIT
172.31.4.140	443	64.39.99.6	53340	TIME_WAIT
172.31.4.140	443	64.39.99.6	53389	TIME_WAIT
172.31.4.140	80	64.39.99.6	60428	TIME_WAIT
172.31.4.140	443	64.39.99.6	53214	TIME_WAIT
172.31.4.140	443	64.39.99.6	53387	TIME_WAIT
172.31.4.140	443	64.39.99.6	53151	TIME_WAIT
172.31.4.140	443	64.39.99.6	53388	TIME_WAIT
172.31.4.140	443	64.39.99.6	53341	TIME_WAIT
127.0.0.1	39552	127.0.0.1	8080	TIME_WAIT
172.31.4.140	873	64.39.99.6	56092	ESTABLISHED
172.31.4.140	443	64.39.99.6	53359	ESTABLISHED
172.31.4.140	443	64.39.99.6	53224	TIME_WAIT
172.31.4.140	443	64.39.99.6	53330	TIME_WAIT
172.31.4.140	80	64.39.99.6	60708	ESTABLISHED
172.31.4.140	22	64.39.99.6	58490	ESTABLISHED
127.0.0.1	39544	127.0.0.1	8080	TIME_WAIT
172.31.4.140	443	64.39.99.6	53334	TIME_WAIT
172.31.4.140	443	64.39.99.6	53328	TIME_WAIT
127.0.0.1	39556	127.0.0.1	8080	TIME_WAIT
172.31.4.140	443	64.39.99.6	53218	TIME_WAIT
127.0.0.1	39568	127.0.0.1	8080	TIME_WAIT
172.31.4.140	80	64.39.99.6	60447	TIME_WAIT
172.31.4.140	443	64.39.99.6	53393	TIME_WAIT
172.31.4.140	443	64.39.99.6	53353	TIME_WAIT
172.31.4.140	443	64.39.99.6	53196	TIME_WAIT
172.31.4.140	443	64.39.99.6	53333	TIME_WAIT
172.31.4.140	443	64.39.99.6	53331	TIME_WAIT
172.31.4.140	80	64.39.99.6	60446	TIME_WAIT
172.31.4.140	443	64.39.99.6	53215	TIME_WAIT
172.31.4.140	443	64.39.99.6	53230	TIME_WAIT
172.31.4.140	443	64.39.99.6	53385	TIME_WAIT
172.31.4.140	80	64.39.99.6	60467	TIME_WAIT
172.31.4.140	443	64.39.99.6	53386	TIME_WAIT
172.31.4.140	443	64.39.99.6	53213	TIME_WAIT
172.31.4.140	443	64.39.99.6	53295	TIME_WAIT
172.31.4.140	443	64.39.99.6	53329	TIME_WAIT
172.31.4.140	443	64.39.99.6	53332	TIME_WAIT

172.31.4.140	443	64.39.99.6	53216	TIME_WAIT
172.31.4.140	443	64.39.99.6	53212	TIME_WAIT
172.31.4.140	80	64.39.99.6	60475	TIME_WAIT
127.0.0.1	8080	127.0.0.1	39514	TIME_WAIT
127.0.0.1	8080	127.0.0.1	39576	TIME_WAIT
127.0.0.1	8080	127.0.0.1	39560	TIME_WAIT
127.0.0.1	8080	127.0.0.1	39510	TIME_WAIT
127.0.0.1	8080	127.0.0.1	39526	TIME_WAIT
127.0.0.1	8080	127.0.0.1	39530	TIME_WAIT
127.0.0.1	8080	127.0.0.1	39572	TIME_WAIT
127.0.0.1	8080	127.0.0.1	39502	TIME_WAIT
127.0.0.1	8080	127.0.0.1	39580	TIME_WAIT
127.0.0.1	8080	127.0.0.1	39534	TIME_WAIT
127.0.0.1	8080	127.0.0.1	39564	TIME_WAIT
127.0.0.1	8080	127.0.0.1	39538	TIME_WAIT
127.0.0.1	8080	127.0.0.1	39522	TIME_WAIT
127.0.0.1	8080	127.0.0.1	39518	TIME_WAIT

1 Internet Protocol version 6 (IPv6) Enabled on Target Host

QID:	45193
Category:	Information gathering
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	07/31/2018
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
Internet Protocol version 6 (IPv6) is the latest revision of the Internet Protocol (IP), the communications protocol that routes traffic across the Internet. It is intended to replace IPv4, which still carries the vast majority of Internet traffic as of 2013.
This QID uses the registry key mentioned in Microsoft KB929852 (http://support.microsoft.com/kb/929852) to determine if IPv6 is enabled.
The detection works in the following way:
1) For Windows 2000,XP,2003
-- Check for existence of key "HKLM\SYSTEM\CurrentControlSet\Services\Tcpip6\Parameters"
2) For Windows Vista or 2008 or Windows 7 or Windows 8 or Windows Server 2012 and Windows RT:
-- It checks the value of "DisabledComponents" for key "HKLM\SYSTEM\CurrentControlSet\Services\Tcpip6\Parameters"
Note: This checks make use of Windows Management Instrumentation(WMI) to list IPv6 Addresses on target.
On UNIX based systems, this QID runs the ifconfig command grepping for IPv6 output.

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:
inet6 addr: fe80::42:2ff:fe23:d042/64 Scope:Link

inet6 addr: fe80::83e:29ff:fe1b:4162/64 Scope:Link
inet6 addr: ::1/128 Scope:Host
inet6 addr: fe80::1404:62ff:fe23:19cf/64 Scope:Link

1 OpenSSL (Open Source toolkit for SSL/TLS) Detected

QID:	45222
Category:	Information gathering
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	07/07/2014
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
OpenSSL is an open-source implementation of the SSL and TLS protocols. OpenSSL is based on SSLeay.
Qualys detected OpenSSL on the host. Please note that in remote detections, security patches may be backported and the displayed version number may not show the correct patch level.

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:
OpenSSL 1.0.2g 1 Mar 2016

1 UNIX Daemon/Services Listed Under Non-Root Users

QID:	45240
Category:	Information gathering
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	07/31/2018
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
This QID displays the daemons/services running under non-root users.

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:
UID PID PPID C STIME TTY TIME CMD
systemd+ 561 1 0 Aug20 ? 00:00:00 /lib/systemd/systemd-timesyncd
syslog 1078 1 0 Aug20 ? 00:00:00 /usr/sbin/rsyslogd -n
daemon 1092 1 0 Aug20 ? 00:00:00 /usr/sbin/atd -f
message+ 1107 1 0 Aug20 ? 00:00:01 /usr/bin/dbus-daemon --system --address=systemd: --nofork --nopidfile --systemd-activation
svc-qlys 1129 32320 0 17:19 pts/1 00:00:00 -bash
svc-qlys 1130 1129 0 17:19 pts/1 00:00:00 ps -ef
www-data 23358 20033 0 Aug20 ? 00:00:03 nginx: worker process
www-data 23359 20033 0 Aug20 ? 00:00:08 nginx: worker process
www-data 25466 25389 0 Aug20 ? 00:00:01 apache2 -DFOREGROUND
www-data 25467 25389 0 Aug20 ? 00:00:00 apache2 -DFOREGROUND
www-data 25468 25389 0 Aug20 ? 00:00:00 apache2 -DFOREGROUND
www-data 25469 25389 0 Aug20 ? 00:00:01 apache2 -DFOREGROUND
www-data 25470 25389 0 Aug20 ? 00:00:00 apache2 -DFOREGROUND
www-data 25471 25389 0 Aug20 ? 00:00:00 apache2 -DFOREGROUND
www-data 25494 25389 0 Aug20 ? 00:00:00 apache2 -DFOREGROUND
ubuntu 32142 1 0 16:43 ? 00:00:00 /lib/systemd/systemd --user
ubuntu 32144 32142 0 16:43 ? 00:00:00 (sd-pam)
ubuntu 32178 32140 0 16:43 ? 00:00:00 sshd: ubuntu@pts/0
ubuntu 32179 32178 0 16:43 pts/0 00:00:00 -bash
svc-qlys 32219 1 0 17:18 ? 00:00:00 /lib/systemd/systemd --user
svc-qlys 32221 32219 0 17:18 ? 00:00:00 (sd-pam)
svc-qlys 32255 32217 0 17:18 ? 00:00:00 sshd: svc-qlys@pts/1
svc-qlys 32320 32255 2 17:19 pts/1 00:00:00 -bash

 1 UNIX Daemon/Services Listed Under Root User

QID:	45241
Category:	Information gathering
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	07/31/2018
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
This QID displays the daemons/services running under the root user.

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

```
root        1    0  0 Aug20 ?        00:00:06 /sbin/init
root        2    0  0 Aug20 ?        00:00:00 [kthreadd]
root        3    2  0 Aug20 ?        00:00:00 [ksoftirqd/0]
root        5    2  0 Aug20 ?        00:00:00 [kworker/0:0H]
root        7    2  0 Aug20 ?        00:00:01 [rcu_sched]
root        8    2  0 Aug20 ?        00:00:00 [rcu_bh]
root        9    2  0 Aug20 ?        00:00:00 [migration/0]
root       10    2  0 Aug20 ?        00:00:00 [watchdog/0]
root       11    2  0 Aug20 ?        00:00:00 [watchdog/1]
root       12    2  0 Aug20 ?        00:00:00 [migration/1]
root       13    2  0 Aug20 ?        00:00:02 [ksoftirqd/1]
root       15    2  0 Aug20 ?        00:00:00 [kworker/1:0H]
root       16    2  0 Aug20 ?        00:00:00 [kdevtmpfs]
root       17    2  0 Aug20 ?        00:00:00 [netns]
root       18    2  0 Aug20 ?        00:00:00 [perf]
root       19    2  0 Aug20 ?        00:00:00 [xenwatch]
root       20    2  0 Aug20 ?        00:00:00 [xenbus]
root       22    2  0 Aug20 ?        00:00:00 [khungtaskd]
root       23    2  0 Aug20 ?        00:00:00 [writeback]
root       24    2  0 Aug20 ?        00:00:00 [ksmd]
root       25    2  0 Aug20 ?        00:00:00 [khugepaged]
root       26    2  0 Aug20 ?        00:00:00 [crypto]
root       27    2  0 Aug20 ?        00:00:00 [kintegrityd]
root       28    2  0 Aug20 ?        00:00:00 [bioset]
root       29    2  0 Aug20 ?        00:00:00 [kblockd]
root       30    2  0 Aug20 ?        00:00:00 [ata_sff]
root       31    2  0 Aug20 ?        00:00:00 [md]
root       32    2  0 Aug20 ?        00:00:00 [devfreq_wq]
root       36    2  0 Aug20 ?        00:00:02 [kswapd0]
root       37    2  0 Aug20 ?        00:00:00 [vmstat]
root       38    2  0 Aug20 ?        00:00:00 [fsnotify_mark]
root       39    2  0 Aug20 ?        00:00:00 [ecryptfs-kthrea]
root       55    2  0 Aug20 ?        00:00:00 [kthrotld]
root       56    2  0 Aug20 ?        00:00:00 [bioset]
root       57    2  0 Aug20 ?        00:00:00 [bioset]
root       58    2  0 Aug20 ?        00:00:00 [bioset]
root       59    2  0 Aug20 ?        00:00:00 [bioset]
root       60    2  0 Aug20 ?        00:00:00 [bioset]
root       61    2  0 Aug20 ?        00:00:00 [bioset]
root       62    2  0 Aug20 ?        00:00:00 [bioset]
root       63    2  0 Aug20 ?        00:00:00 [bioset]
root       64    2  0 Aug20 ?        00:00:00 [bioset]
root       65    2  0 Aug20 ?        00:00:00 [bioset]
root       66    2  0 Aug20 ?        00:00:00 [bioset]
root       67    2  0 Aug20 ?        00:00:00 [bioset]
root       68    2  0 Aug20 ?        00:00:00 [bioset]
root       69    2  0 Aug20 ?        00:00:00 [bioset]
root       70    2  0 Aug20 ?        00:00:00 [bioset]
root       71    2  0 Aug20 ?        00:00:00 [bioset]
root       72    2  0 Aug20 ?        00:00:00 [bioset]
root       73    2  0 Aug20 ?        00:00:00 [bioset]
root       74    2  0 Aug20 ?        00:00:00 [bioset]
root       75    2  0 Aug20 ?        00:00:00 [bioset]
root       76    2  0 Aug20 ?        00:00:00 [bioset]
root       77    2  0 Aug20 ?        00:00:00 [bioset]
root       78    2  0 Aug20 ?        00:00:00 [bioset]
root       79    2  0 Aug20 ?        00:00:00 [bioset]
root       80    2  0 Aug20 ?        00:00:00 [scsi_eh_0]
root       81    2  0 Aug20 ?        00:00:00 [scsi_tmf_0]
root       82    2  0 Aug20 ?        00:00:00 [scsi_eh_1]
root       83    2  0 Aug20 ?        00:00:00 [scsi_tmf_1]
root       85    2  0 Aug20 ?        00:00:00 [bioset]
root       86    2  0 Aug20 ?        00:00:00 [bioset]
root       90    2  0 Aug20 ?        00:00:00 [ipv6_addrconf]
root      104    2  0 Aug20 ?        00:00:00 [deferwq]
root      265    2  0 Aug20 ?        00:00:00 [raid5wq]
root      295    2  0 Aug20 ?        00:00:00 [bioset]
root      314    2  0 Aug20 ?        00:00:00 [jbd2/xvda1-8]
root      315    2  0 Aug20 ?        00:00:00 [ext4-rsv-conver]
root      363    2  0 Aug20 ?        00:00:00 [kworker/0:1H]
root      381    2  0 Aug20 ?        00:00:00 [iscsi_eh]
```

```
root       393     2  0 Aug20 ?        00:00:00 [ib_addr]
root       398     2  0 Aug20 ?        00:00:00 [ib_mcast]
root       399     2  0 Aug20 ?        00:00:00 [ib_nl_sa_wq]
root       401     1  0 Aug20 ?        00:00:00 /lib/systemd/systemd-journald
root       404     2  0 Aug20 ?        00:00:00 [ib_cm]
root       405     2  0 Aug20 ?        00:00:00 [iw_cm_wq]
root       406     2  0 Aug20 ?        00:00:00 [rdma_cm]
root       418     2  0 Aug20 ?        00:00:00 [kauditd]
root       437     1  0 Aug20 ?        00:00:00 /sbin/lvmetad -f
root       469     1  0 Aug20 ?        00:00:00 /lib/systemd/systemd-udevd
root       504     2  0 Aug20 ?        00:00:00 [loop0]
root       510     2  0 Aug20 ?        00:00:00 [loop1]
root       651     2  0 17:19 ?       00:00:00 [kworker/u30:0]
root       951     1  0 Aug20 ?        00:00:00 /sbin/dhclient -1 -v -pf /run/dhclient.eth0.pid -lf /var/lib/dhcp/dhclient.eth0.leases -I -df /var/lib/dhcp/
dhclient6.eth0.leases eth0
root      1071 25738  0 17:19 ?        00:00:00 /usr/bin/rsync --daemon --no-detach
root      1079     1  0 Aug20 ?        00:00:00 /lib/systemd/systemd-logind
root      1080     1  0 Aug20 ?        00:00:01 /usr/lib/accountsservice/accounts-daemon
root      1089     1  0 Aug20 ?        00:00:00 /usr/sbin/cron -f
root      1125     1  0 Aug20 ?        00:00:00 /usr/sbin/acpid
root      1136     1  0 Aug20 ?        00:00:00 /usr/bin/lxcfs /var/lib/lxcfs/
svc-qlys  1137  1134  0 17:19 pts/1    00:00:00 grep --color=auto root
root      1164     2  0 Aug20 ?        00:00:00 [kworker/1:1H]
root      1186     1  0 Aug20 ?        00:00:00 /usr/lib/policykit-1/polkitd --no-debug
root      1190     1  0 Aug20 ?        00:00:00 /sbin/mdadm --monitor --pid-file /run/mdadm/monitor.pid --daemonise --scan --syslog
root      1241     1  0 Aug20 ?        00:00:03 /usr/sbin/irqbalance --pid=/var/run/irqbalance.pid
root      1267     1  0 Aug20 ttyS0    00:00:00 /sbin/agetty --keep-baud 115200 38400 9600 ttyS0 vt220
root      1274     1  0 Aug20 tty1     00:00:00 /sbin/agetty --noclear tty1 linux
root      1303     1  0 Aug20 ?        00:00:00 /usr/sbin/sshd -D
root     11021     1  0 Aug20 ?        00:02:36 /usr/bin/dockerd -H fd://
root     11030 11021  0 Aug20 ?        00:04:02 docker-containerd --config /var/run/docker/containerd/containerd.toml
root     15849     1  0 Aug20 ?        00:00:02 /sbin/iscsid
root     15850     1  0 Aug20 ?        00:00:11 /sbin/iscsid
root     20033     1  0 Aug20 ?        00:00:00 nginx: master process /usr/sbin/nginx -g daemon on; master_process on;
root     22292     2  0 Aug20 ?        00:00:00 [jbd2/xvdb-8]
root     22293     2  0 Aug20 ?        00:00:00 [ext4-rsv-conver]
root     25360 11021  0 Aug20 ?        00:00:04 /usr/bin/docker-proxy -proto tcp -host-ip 0.0.0.0 -host-port 8080 -container-ip 172.18.0.2 -container-
port 80
root     25370 11030  0 Aug20 ?        00:00:02 docker-containerd-shim -namespace moby -workdir /var/lib/docker/containerd/daemon/io.containerd.
runtime.v1.linux/moby/edf3e1a8254ea0328de9f8560e165e47360da21bd63864da981275df74ce4a2f -address /var/run/docker/containerd/docker-
containerd.sock -containerd-binary /usr/bin/docker-containerd -runtime-root /var/run/docker/runtime-runc
root     25389 25370  0 Aug20 ?        00:00:03 apache2 -DFOREGROUND
root     25738     1  0 Aug20 ?        00:00:00 /usr/bin/rsync --daemon --no-detach
root     26199     2  0 Aug20 ?        00:00:00 [loop2]
root     26217     1  0 Aug20 ?        00:00:04 /usr/lib/snapd/snapd
root     26341     2  0 Aug20 ?        00:00:00 [loop3]
root     26452     1  0 Aug20 ?        00:00:00 /snap/amazon-ssm-agent/495/amazon-ssm-agent
root     29303     2  0 14:45 ?        00:00:00 [kworker/0:3]
root     30890     2  0 14:51 ?        00:00:00 [kworker/u30:2]
root     31861     2  0 14:52 ?        00:00:00 [kworker/u30:3]
root     31999     2  0 16:05 ?        00:00:00 [kworker/1:3]
root     32037     2  0 16:43 ?        00:00:00 [kworker/1:0]
root     32134     2  0 16:43 ?        00:00:00 [kworker/0:0]
root     32140  1303  0 16:43 ?        00:00:00 sshd: ubuntu [priv]
root     32217  1303  0 17:18 ?        00:00:00 sshd: svc-qlys [priv]
root     32220     2  0 17:18 ?        00:00:00 [kworker/0:1]
```

1 Content of the apt repositories

QID:	45293
Category:	Information gathering
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	07/02/2018
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

The /etc/apt/sources.list contains a list of configured APT data sources. The /etc/apt/sources.list.d directory provides a way to add sources.list entries in separate files. The information available from these configured sources is acquired by apt-get update to download necessary update files.
NOTE: This QID will return blank results if the /etc/apt/sources.list or /etc/apt/sources.list.d/* files exist, but do not have any content.
QID Detection Logic:
This authenticated QID prints the contents of the /etc/apt/sources.list and cat /etc/apt/sources.list/* files.

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:
Contents of the sources.list file:

Note, this file is written by cloud-init on first boot of an instance
modifications made here will not survive a re-bundle.
if you wish to make changes you can:
a.) add 'apt_preserve_sources_list: true' to /etc/cloud/cloud.cfg
or do the same in user-data
b.) add sources in /etc/apt/sources.list.d
c.) make changes to template file /etc/cloud/templates/sources.list.tmpl

See http://help.ubuntu.com/community/UpgradeNotes for how to upgrade to
newer versions of the distribution.
deb http://us-east-1.ec2.archive.ubuntu.com/ubuntu/ xenial main restricted
deb-src http://us-east-1.ec2.archive.ubuntu.com/ubuntu/ xenial main restricted

Major bug fix updates produced after the final release of the
distribution.
deb http://us-east-1.ec2.archive.ubuntu.com/ubuntu/ xenial-updates main restricted
deb-src http://us-east-1.ec2.archive.ubuntu.com/ubuntu/ xenial-updates main restricted

N.B. software from this repository is ENTIRELY UNSUPPORTED by the Ubuntu
team. Also, please note that software in universe WILL NOT receive any
review or updates from the Ubuntu security team.
deb http://us-east-1.ec2.archive.ubuntu.com/ubuntu/ xenial universe
deb-src http://us-east-1.ec2.archive.ubuntu.com/ubuntu/ xenial universe
deb http://us-east-1.ec2.archive.ubuntu.com/ubuntu/ xenial-updates universe
deb-src http://us-east-1.ec2.archive.ubuntu.com/ubuntu/ xenial-updates universe

N.B. software from this repository is ENTIRELY UNSUPPORTED by the Ubuntu
team, and may not be under a free licence. Please satisfy yourself as to
your rights to use the software. Also, please note that software in
multiverse WILL NOT receive any review or updates from the Ubuntu
security team.
deb http://us-east-1.ec2.archive.ubuntu.com/ubuntu/ xenial multiverse
deb-src http://us-east-1.ec2.archive.ubuntu.com/ubuntu/ xenial multiverse
deb http://us-east-1.ec2.archive.ubuntu.com/ubuntu/ xenial-updates multiverse
deb-src http://us-east-1.ec2.archive.ubuntu.com/ubuntu/ xenial-updates multiverse

N.B. software from this repository may not have been tested as
extensively as that contained in the main release, although it includes
newer versions of some applications which may provide useful features.
Also, please note that software in backports WILL NOT receive any review
or updates from the Ubuntu security team.
deb http://us-east-1.ec2.archive.ubuntu.com/ubuntu/ xenial-backports main restricted universe multiverse
deb-src http://us-east-1.ec2.archive.ubuntu.com/ubuntu/ xenial-backports main restricted universe multiverse

deb http://security.ubuntu.com/ubuntu xenial-security main restricted
deb-src http://security.ubuntu.com/ubuntu xenial-security main restricted
deb http://security.ubuntu.com/ubuntu xenial-security universe
deb-src http://security.ubuntu.com/ubuntu xenial-security universe
deb http://security.ubuntu.com/ubuntu xenial-security multiverse

deb-src http://security.ubuntu.com/ubuntu xenial-security multiverse

Uncomment the following two lines to add software from Canonical's
'partner' repository.
This software is not part of Ubuntu, but is offered by Canonical and the
respective vendors as a service to Ubuntu users.
deb http://archive.canonical.com/ubuntu xenial partner
deb-src http://archive.canonical.com/ubuntu xenial partner

Contents of the sources.list.d file:

deb http://ppa.launchpad.net/certbot/certbot/ubuntu xenial main
deb-src http://ppa.launchpad.net/certbot/certbot/ubuntu xenial main
deb [arch=amd64] https://download.docker.com/linux/ubuntu xenial stable
deb [arch=amd64] https://download.docker.com/linux/ubuntu xenial stable

 1 Open UDP Services List

QID:	82004
Category:	TCP/IP
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	07/11/2005
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
A port scanner was used to draw a map of all the UDP services on this host that can be accessed from the Internet.
Note that if the host is behind a firewall, there is a small chance that the list includes a few ports that are filtered or blocked by the firewall but are not actually open on the target host. This (false positive on UDP open ports) may happen when the firewall is configured to reject UDP packets for most (but not all) ports with an ICMP Port Unreachable packet. This may also happen when the firewall is configured to allow UDP packets for most (but not all) ports through and filter/block/drop UDP packets for only a few ports. Both cases are uncommon.

IMPACT:
Unauthorized users can exploit this information to test vulnerabilities in each of the open services.

SOLUTION:
Shut down any unknown or unused service on the list. If you have difficulty working out which service is provided by which process or program, contact your provider's support team. For more information about commercial and open-source Intrusion Detection Systems available for detecting port scanners of this kind, visit the CERT Web site (http://www.cert.org).

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

Port	IANA Assigned Ports/Services	Description	Service Detected
68	bootpc	Bootstrap Protocol Client	unknown

 1 Open TCP Services List

QID:	82023
Category:	TCP/IP
CVE ID:	-
Vendor Reference:	-

Bugtraq ID: -
Service Modified: 06/15/2009
User Modified: -
Edited: No
PCI Vuln: No

THREAT:
The port scanner enables unauthorized users with the appropriate tools to draw a map of all services on this host that can be accessed from the Internet. The test was carried out with a "stealth" port scanner so that the server does not log real connections.
The Results section displays the port number (Port), the default service listening on the port (IANA Assigned Ports/Services), the description of the service (Description) and the service that the scanner detected using service discovery (Service Detected).

IMPACT:
Unauthorized users can exploit this information to test vulnerabilities in each of the open services.

SOLUTION:
Shut down any unknown or unused service on the list. If you have difficulty figuring out which service is provided by which process or program, contact your provider's support team. For more information about commercial and open-source Intrusion Detection Systems available for detecting port scanners of this kind, visit the CERT Web site (http://www.cert.org).

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

Port	IANA Assigned Ports/Services	Description	Service Detected	OS On Redirected Port
22	ssh	SSH Remote Login Protocol	ssh	
80	www-http	World Wide Web HTTP	http	
443	https	http protocol over TLS/SSL	http over ssl	
873	rsync	rsync	rsyncd	
8080	http-alt	HTTP Alternate (see port 80)	http	Ubuntu / Fedora / Tiny Core Linux / Linux 3.x


1 Operating Systems Detected on Redirected TCP Open Ports

QID: 82038
Category: TCP/IP
CVE ID: -
Vendor Reference: -
Bugtraq ID: -
Service Modified: 04/08/2003
User Modified: -
Edited: No
PCI Vuln: No

THREAT:
A redirected TCP open port is a port that is not native to the host scanned. It may belong to another host that is either closer to or further away from the scanner.
The service detected one or more redirected TCP open ports and finger-printed the operating systems these ports belong to.
When a redirected TCP open port is detected, it may be difficult for the service to determine whether the port is native to the host. Ports displayed as "redirected" may actually be native and vice versa.

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

Redirected Port	OS
8080	Ubuntu / Fedora / Tiny Core Linux / Linux 3.x

1 ICMP Replies Received

QID:	82040
Category:	TCP/IP
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	01/16/2003
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
ICMP (Internet Control and Error Message Protocol) is a protocol encapsulated in IP packets. ICMP's principal purpose is to provide a protocol layer that informs gateways of the inter-connectivity and accessibility of other gateways or hosts.
We have sent the following types of packets to trigger the host to send us ICMP replies:
Echo Request (to trigger Echo Reply)
Timestamp Request (to trigger Timestamp Reply)
Address Mask Request (to trigger Address Mask Reply)
UDP Packet (to trigger Port Unreachable Reply)
IP Packet with Protocol >= 250 (to trigger Protocol Unreachable Reply)
Listed in the "Result" section are the ICMP replies that we have received.

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

ICMP Reply Type	Triggered By	Additional Information
Echo (type=0 code=0)	Echo Request	Echo Reply
Time Stamp (type=14 code=0)	Time Stamp Request	17:17:20 GMT
Unreachable (type=3 code=3)	UDP Port 62398	Port Unreachable
Unreachable (type=3 code=3)	UDP Port 1	Port Unreachable
Unreachable (type=3 code=3)	UDP Port 1194	Port Unreachable
Unreachable (type=3 code=3)	UDP Port 2002	Port Unreachable
Unreachable (type=3 code=3)	UDP Port 80	Port Unreachable
Unreachable (type=3 code=3)	UDP Port 1701	Port Unreachable
Unreachable (type=3 code=3)	UDP Port 517	Port Unreachable
Unreachable (type=3 code=3)	UDP Port 3527	Port Unreachable
Unreachable (type=3 code=3)	UDP Port 7778	Port Unreachable
Unreachable (type=3 code=3)	UDP Port 13	Port Unreachable

1 Degree of Randomness of TCP Initial Sequence Numbers

QID:	82045
Category:	TCP/IP
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	11/19/2004
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
TCP Initial Sequence Numbers (ISNs) obtained in the SYNACK replies from the host are analyzed to determine how random they are. The average change between subsequent ISNs and the standard deviation from the average are displayed in the RESULT section. Also included is the degree of difficulty for exploitation of the TCP ISN generation scheme used by the host.

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:
Average change between subsequent TCP initial sequence numbers is 1130325087 with a standard deviation of 692190931. These TCP initial sequence numbers were triggered by TCP SYN probes sent to the host at an average rate of 1/(6260 microseconds). The degree of difficulty to exploit the TCP initial sequence number generation scheme is: hard.

 1 IP ID Values Randomness

QID:	82046
Category:	TCP/IP
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	07/27/2006
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
The values for the identification (ID) field in IP headers in IP packets from the host are analyzed to determine how random they are. The changes between subsequent ID values for either the network byte ordering or the host byte ordering, whichever is smaller, are displayed in the RESULT section along with the duration taken to send the probes. When incremental values are used, as is the case for TCP/IP implementation in many operating systems, these changes reflect the network load of the host at the time this test was conducted.
Please note that for reliability reasons only the network traffic from open TCP ports is analyzed.

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

IP ID changes observed (network order) for port 22: 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0
Duration: 26 milli seconds

1 Unix User List

QID:	105085
Category:	Security Policy
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	06/14/2017
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
The report sections catalogs users found on the host system.

IMPACT:
Make sure that the user list adheres to your security policy, so it's not possible for unauthorized users to launch attacks from the host.

SOLUTION:
Remove or modify users to comply with your security policy.

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

root:0
daemon:1
bin:2
sys:3
sync:4
games:5
man:6
lp:7
mail:8
news:9
uucp:10
proxy:13
www-data:33
backup:34
list:38
irc:39
gnats:41
nobody:65534
systemd-timesync:100
systemd-network:101
systemd-resolve:102

systemd-bus-proxy:103
syslog:104
_apt:105
lxd:106
messagebus:107
uuidd:108
dnsmasq:109
sshd:110
pollinate:111
ubuntu:1000
matrix:1001
svc-qlys:1002

1 "At" Command Configuration

QID:	105143
Category:	Security Policy
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	03/22/2005
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
The "At" command allows users to run executables on the system at arbitrary future times. Depending on site policy, this could be considered as a security threat.
The superuser may use these commands in any case. For other users, permission to use the "at" command is determined by the files /etc/at.allow and /etc/at.deny.
If the file /etc/at.allow exists, only usernames mentioned in the file are allowed to use the "at" command. If /etc/at.allow does not exist, /etc/at.deny is checked, and every username not mentioned in it is then allowed to use the "at" command. If neither file exists, only the superuser is allowed use of the "at" command. An empty /etc/at.deny means that all users are allowed access. This is the default configuration.
Note: The Results section is formatted in the following way: It first lists the "ls -la" permissions of any /etc/at.allow or /etc/at.deny files on the target. If present, the contents of the files are "cat"ed (at.deny is typically empty, so it will show up as white space). If the "ls -la" line and the contents of the corresponding file are not shown, it means the file does not exist on the target.

IMPACT:
N/A

SOLUTION:
Please check the configuration to ensure only authorized users of the system have access to the "at" command.

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:
-rw-r----- 1 root daemon 144 Jan 14 2016 /etc/at.deny

1 Linux - Network Parameter - tcp_max_syn_backlog Value

QID:	105301
Category:	Security Policy
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	05/01/2006
User Modified:	-

Edited:	No
PCI Vuln:	No

THREAT:
The value specifies the maximum number of remembered connection requests which have not yet received an acknowledgment from the connecting client.

IMPACT:
N/A

SOLUTION:
The Center for Internet Security (http://www.cisecurity.com) recommends that the value be set to 4096.
This value can be enabled in Linux by editing the /etc/sysctl.conf to reflect the following:

net.ipv4.tcp_max_syn_backlog = 4096

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:
128

1 Linux - Network Parameter - accept_source_route Value

QID:	105303
Category:	Security Policy
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	05/11/2006
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
The accept_source_route value specifies how to handle packets with the SSR option set.
The conf/all/accept_source_route value is boolean:
0 - Do not accept packets
1 - Accept packets

IMPACT:
N/A

SOLUTION:
The Center for Internet Security (http://www.cisecurity.com) recommends that the value be set to 0.
This value can be enabled in Linux by editing the /etc/sysctl.conf to reflect the following:

net.ipv4.conf.all.accept_source_route = 0
net.ipv4.conf.default.accept_source_route = 0

COMPLIANCE:
Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:
/proc/sys/net/ipv4/conf/br-ede829f66747/accept_source_route:1
/proc/sys/net/ipv4/conf/default/accept_source_route:1
/proc/sys/net/ipv4/conf/docker0/accept_source_route:1
/proc/sys/net/ipv4/conf/eth0/accept_source_route:1
/proc/sys/net/ipv4/conf/veth8a12c3e/accept_source_route:1

1 Linux - Network Parameter - accept_redirects Value

QID:	105304
Category:	Security Policy
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	05/11/2006
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
The accept_redirects variable specifies if the system should accept ICMP redirect messages.
The conf/all/accept_redirects value is boolean:
0 - Do not accept ICMP redirect messages.
1 - Accept ICMP redirect messages.

IMPACT:
N/A

SOLUTION:
The Center for Internet Security (http://www.cisecurity.com) recommends that the value be set to 0.
This value can be enabled in Linux by editing the /etc/sysctl.conf to reflect the following:

net.ipv4.conf.all.accept_redirects = 0
net.ipv4.conf.default.accept_redirects = 0

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:
/proc/sys/net/ipv4/conf/br-ede829f66747/accept_redirects:1
/proc/sys/net/ipv4/conf/default/accept_redirects:1
/proc/sys/net/ipv4/conf/docker0/accept_redirects:1
/proc/sys/net/ipv4/conf/eth0/accept_redirects:1
/proc/sys/net/ipv4/conf/veth8a12c3e/accept_redirects:1

1 Linux - Network Parameter - secure_redirects Value

QID:	105306
Category:	Security Policy
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-

Service Modified:	05/11/2006
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
The secure_redirects variable specifies if the system should accept ICMP redirect messages from any host, anywhere.
The conf/all/secure_redirects value is boolean:
0 - Accept ICMP redirect messages from any host.
1 - Accept ICMP redirect messages from gateways listed in default gateway list.

IMPACT:
N/A

SOLUTION:
The Center for Internet Security (http://www.cisecurity.com) recommends that the value be set to 0.
This value can be enabled in Linux by editing the /etc/sysctl.conf to reflect the following:

net.ipv4.conf.all.secure_redirects = 0
net.ipv4.conf.default.secure_redirects = 0

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:
/proc/sys/net/ipv4/conf/all/secure_redirects:1
/proc/sys/net/ipv4/conf/br-ede829f66747/secure_redirects:1
/proc/sys/net/ipv4/conf/default/secure_redirects:1
/proc/sys/net/ipv4/conf/docker0/secure_redirects:1
/proc/sys/net/ipv4/conf/eth0/secure_redirects:1
/proc/sys/net/ipv4/conf/veth8a12c3e/secure_redirects:1

 1 Unix Environment Variables

QID:	115041
Category:	Local
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	01/10/2005
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
The result section shows environment variables on the target machine.

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:
XDG_SESSION_ID=63
TERM=vt100
SHELL=/bin/bash
SSH_CLIENT=64.39.99.6 44798 22
SSH_TTY=/dev/pts/1
USER=svc-qlys
LS_COLORS=rs=0:di=01;34:ln=01;36:mh=00:pi=40;33:so=01;35:do=01;35:bd=40;33;01:cd=40;33;01:or=40;31;01:mi=00:su=37;41:sg=30;43:
ca=30;41:tw=30;42:ow=34;42:st=37;44:ex=01;32:*.tar=01;31:*.tgz=01;31:*.arc=01;31:*.arj=01;31:*.taz=01;31:*.lha=01;31:*.lz4=01;31:*.lzh=01;31:*.
lzma=01;31:*.tlz=01;31:*.txz=01;31:*.tzo=01;31:*.t7z=01;31:*.zip=01;31:*.z=01;31:*.Z=01;31:*.dz=01;31:*.gz=01;31:*.lrz=01;31:*.lz=01;31:*.
lzo=01;31:*.xz=01;31:*.bz2=01;31:*.bz=01;31:*.tbz=01;31:*.tbz2=01;31:*.tz=01;31:*.deb=01;31:*.rpm=01;31:*.jar=01;31:*.war=01;31:*.ear=01;31:*.
sar=01;31:*.rar=01;31:*.alz=01;31:*.ace=01;31:*.zoo=01;31:*.cpio=01;31:*.7z=01;31:*.rz=01;31:*.cab=01;31:*.jpg=01;35:*.jpeg=01;35:*.gif=01;35:*.
bmp=01;35:*.pbm=01;35:*.pgm=01;35:*.ppm=01;35:*.tga=01;35:*.xbm=01;35:*.xpm=01;35:*.tif=01;35:*.tiff=01;35:*.png=01;35:*.svg=01;35:*.
svgz=01;35:*.mng=01;35:*.pcx=01;35:*.mov=01;35:*.mpg=01;35:*.mpeg=01;35:*.m2v=01;35:*.mkv=01;35:*.webm=01;35:*.ogm=01;35:*.
mp4=01;35:*.m4v=01;35:*.mp4v=01;35:*.vob=01;35:*.qt=01;35:*.nuv=01;35:*.wmv=01;35:*.asf=01;35:*.rm=01;35:*.rmvb=01;35:*.flc=01;35:*.
avi=01;35:*.fli=01;35:*.flv=01;35:*.gl=01;35:*.dl=01;35:*.xcf=01;35:*.xwd=01;35:*.yuv=01;35:*.cgm=01;35:*.emf=01;35:*.ogv=01;35:*.ogx=01;35:*.
aac=00;36:*.au=00;36:*.flac=00;36:*.m4a=00;36:*.mid=00;36:*.midi=00;36:*.mka=00;36:*.mp3=00;36:*.mpc=00;36:*.ogg=00;36:*.ra=00;36:*.
wav=00;36:*.oga=00;36:*.opus=00;36:*.spx=00;36:*.xspf=00;36:
MAIL=/var/mail/svc-qlys
PATH=/home/svc-qlys/bin:/home/svc-qlys/.local/bin:/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin:/usr/games:/usr/local/games:/snap/bin
PWD=/home/svc-qlys
LANG=en_US.UTF-8
SHLVL=1
HOME=/home/svc-qlys
ORIG_PATH=/home/svc-qlys/bin:/home/svc-qlys/.local/bin:/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin:/usr/games:/usr/local/games:/snap/
bin
LOGNAME=svc-qlys
XDG_DATA_DIRS=/usr/local/share:/usr/share:/var/lib/snapd/desktop
SSH_CONNECTION=64.39.99.6 44798 172.31.4.140 22
LESSOPEN=| /usr/bin/lesspipe %s
XDG_RUNTIME_DIR=/run/user/1002
LESSCLOSE=/usr/bin/lesspipe %s %s
_=/usr/bin/env

1 File System Information

QID:	115044
Category:	Local
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	01/10/2005
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
The result section lists file systems currently supported by the target host.

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:
nodev sysfs
nodev rootfs
nodev ramfs
nodev bdev
nodev proc
nodev cpuset
nodev cgroup
nodev tmpfs
nodev devtmpfs
nodev debugfs
nodev tracefs
nodev securityfs
nodev sockfs
nodev bpf
nodev pipefs
nodev devpts
 ext3
 ext2
 ext4
 squashfs
nodev hugetlbfs
 vfat
nodev ecryptfs
 fuseblk
nodev fuse
nodev fusectl
nodev pstore
nodev mqueue
 btrfs
nodev autofs
nodev aufs
nodev overlayfs
nodev overlay

 1 Hard Drive Device Information

QID:	115045
Category:	Local
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	01/10/2005
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
The results section displays the target system's current hard drives.

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

```
LABEL=cloudimg-rootfs /  ext4 defaults,discard 0 0
/dev/xvdb  /mnt/data ext4 defaults 0 0
```

1 Disk Usage Information

QID:	115046
Category:	Local
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	01/10/2005
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
The result section shows the amount of free space left on currently mounted drives.

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

```
Filesystem     1K-blocks     Used Available Use% Mounted on
udev             2014528        0   2014528   0% /dev
tmpfs             404508    11024    393484   3% /run
/dev/xvda1      16197524  3818592  12362548  24% /
tmpfs            2022524        0   2022524   0% /dev/shm
tmpfs               5120        0      5120   0% /run/lock
tmpfs            2022524        0   2022524   0% /sys/fs/cgroup
/dev/loop0         12928    12928         0 100% /snap/amazon-ssm-agent/295
/dev/loop1         89088    89088         0 100% /snap/core/4830
/dev/xvdb      103081248 10039868  87782116  11% /mnt/data
/dev/loop2         89088    89088         0 100% /snap/core/5145
/dev/loop3         13056    13056         0 100% /snap/amazon-ssm-agent/495
tmpfs             404508        0    404508   0% /run/user/1000
tmpfs             404508        0    404508   0% /run/user/1002
```

1 Processor Information for Unix Target

QID:	115048
Category:	Local
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	01/03/2018
User Modified:	-
Edited:	No

PCI Vuln: No

THREAT:
The result section displays the processor information of the Unix based host system.
QID Detection Logic:
This authenticated QID runs the command: "cat /proc/cpuinfo".

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:
processor: 0
vendor_id: GenuineIntel
cpu family: 6
model: 79
model name: Intel(R) Xeon(R) CPU E5-2686 v4 @ 2.30GHz
stepping: 1
microcode: 0xb00002a
cpu MHz: 2300.032
cache size: 46080 KB
physical id: 0
siblings: 2
core id: 0
cpu cores: 2
apicid: 0
initial apicid: 0
fpu: yes
fpu_exception: yes
cpuid level: 13
wp: yes
flags: fpu vme de pse tsc msr pae mce cx8 apic sep mtrr pge mca cmov pat pse36 clflush mmx fxsr sse sse2 ht syscall nx rdtscp lm constant_tsc rep_good nopl xtopology eagerfpu pni pclmulqdq ssse3 fma cx16 pcid sse4_1 sse4_2 x2apic movbe popcnt tsc_deadline_timer aes xsave avx f16c rdrand hypervisor lahf_lm abm invpcid_single kaiser fsgsbase bmi1 avx2 smep bmi2 erms invpcid xsaveopt
bugs: cpu_meltdown spectre_v1 spectre_v2 spec_store_bypass l1tf
bogomips: 4600.06
clflush size: 64
cache_alignment: 64
address sizes: 46 bits physical, 48 bits virtual
power management:

processor: 1
vendor_id: GenuineIntel
cpu family: 6
model: 79
model name: Intel(R) Xeon(R) CPU E5-2686 v4 @ 2.30GHz
stepping: 1
microcode: 0xb00002a
cpu MHz: 2300.032
cache size: 46080 KB
physical id: 0
siblings: 2
core id: 1
cpu cores: 2
apicid: 2
initial apicid: 2
fpu: yes
fpu_exception: yes

cpuid level: 13
wp: yes
flags: fpu vme de pse tsc msr pae mce cx8 apic sep mtrr pge mca cmov pat pse36 clflush mmx fxsr sse sse2 ht syscall nx rdtscp lm constant_tsc rep_good nopl xtopology eagerfpu pni pclmulqdq ssse3 fma cx16 pcid sse4_1 sse4_2 x2apic movbe popcnt tsc_deadline_timer aes xsave avx f16c rdrand hypervisor lahf_lm abm invpcid_single kaiser fsgsbase bmi1 avx2 smep bmi2 erms invpcid xsaveopt
bugs: cpu_meltdown spectre_v1 spectre_v2 spec_store_bypass l1tf
bogomips: 4600.06
clflush size: 64
cache_alignment: 64
address sizes: 46 bits physical, 48 bits virtual
power management:

 1 Memory Information

QID:	115049
Category:	Local
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	03/22/2005
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
The results section shows the total amount of free and used physical memory and swap space on the host system in megabytes. It also shows buffers
and cache consumed by the kernel.

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

total	used	free	shared	buff/cache	available
Mem:	3950	183	164	19	3602	3423
Swap:	0	0	0			
Total:	3950	183	164			

 1 cron.deny File Does Not Exist

QID:	115064
Category:	Local
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	06/23/2005
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
The "cron.deny" file was not found on this system.
The cron daemon runs shell commands at specified dates and times. It is executed upon system initialization and remains active while the system is operating in multi-user mode.
When the crontab command is invoked, it examines the files "cron.deny" and "cron.allow" in the system's cron directory to grant or revoke the modification of the crontab spool file. If a username appears in the "cron.allow" file, the crontab command may be executed. If that file does not exist and the user's name does not appear in the "cron.deny" file, then cron can be used.

IMPACT:
cron can potentially be invoked by users for whom it is not intended.

SOLUTION:
Check to be sure that the absence of the "cron.deny" file is in compliance with your organization's security policy.

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:
No results available

1 cron.allow File Does Not Exist

QID:	115065
Category:	Local
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	06/23/2005
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
The "cron.allow" file was not found on this system.
The cron daemon runs shell commands at specified dates and times. It is executed upon system initialization and remains active while the system is operating in multi-user mode.
When the crontab command is invoked, it examines the files "cron.deny" and "cron.allow" in the system's cron directory to grant or revoke the modification of the crontab spool file. If a username appears in the "cron.allow" file, the crontab command may be executed. If that file does not exist and the user's name does not appear in the "cron.deny" file, then cron can be used.

IMPACT:
cron can potentially be invoked by users for whom it is not intended.

SOLUTION:
Check to be sure that the absence of the "cron.allow" file is in compliance with your organization's security policy.

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:
No results available

1 daemon.notice Entry Missing in syslog.conf

QID:	115068
Category:	Local
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	07/19/2005
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
The file /etc/syslog.conf contains information used by the system log daemon (syslogd) to forward a system message to appropriate log files and/or users. An entry of the form:
daemon.notice[Tab]logfile
ensures that all conditions involving daemons (such as ftpd) that are not error conditions are logged in a logfile. This entry was found to be missing from the syslog.conf file.

IMPACT:
N/A

SOLUTION:
Ensure that the absence of the daemon.notice entry is in compliance with your organization's security policy.

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:
grep: /etc/syslog.conf: No such file or directory

1 User Does Not Have Permission to Read the Shadow File

QID:	121390
Category:	Local
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	02/12/2017
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
The /etc/shadow Linux file stores actual password in encrypted format for a user's account. It also contains password aging controls. All fields are separated by a colon (:).
The current authenticated scan does not have permissions to read the shadow file.

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:
awk: fatal: cannot open file `/etc/shadow' for reading (Permission denied)

1 Docker Version Detected

QID:	123783
Category:	Local
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	05/24/2018
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
Docker is an open-source project that automates the deployment of applications inside software containers, by providing an additional layer of abstraction and automation of operating-system-level virtualization on Linux.
Docker has been detected on the remote system.
QID Detection Logic:
Windows: Presence of a Docker installation is retrieved from the HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{05BD04E9-4AB5-46AC-891E-60EA8FD57D56}_is1 registry key.
Unix: Presence of a Docker installation is detected by running the "docker version" command.
Unauthenticated: Presence of a Docker installation is detected by making requests to the /version endpoint.

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:
Got permission denied while trying to connect to the Docker daemon socket at unix:///var/run/docker.sock: Get http://%2Fvar%2Frun%2Fdocker.sock/v1.38/version: dial unix /var/run/docker.sock: connect: permission denied

1 Interface and IP Address List

QID:	123816
Category:	Local
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	08/17/2018
User Modified:	-

Edited:	No
PCI Vuln:	No

THREAT:
List of Interfaces and IP addresses configured on the scanned host.
QID Detection Logic (Authenticated):
This QID executes ifconfig, netstat, lanscan commands.

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

```
br-ede829f66747 Link encap:Ethernet  HWaddr 02:42:02:23:d0:42
        inet addr:172.18.0.1  Bcast:172.18.255.255  Mask:255.255.0.0
        inet6 addr: fe80::42:2ff:fe23:d042/64 Scope:Link
docker0   Link encap:Ethernet  HWaddr 02:42:44:4c:08:b3
        inet addr:172.17.0.1  Bcast:172.17.255.255  Mask:255.255.0.0
eth0      Link encap:Ethernet  HWaddr 0a:3e:29:1b:41:62
        inet addr:172.31.4.140  Bcast:172.31.15.255  Mask:255.255.240.0
        inet6 addr: fe80::83e:29ff:fe1b:4162/64 Scope:Link
lo        Link encap:Local Loopback
        inet addr:127.0.0.1  Mask:255.0.0.0
        inet6 addr: ::1/128 Scope:Host
veth8a12c3e Link encap:Ethernet  HWaddr 16:04:62:23:19:cf
        inet6 addr: fe80::1404:62ff:fe23:19cf/64 Scope:Link
```

 1 ARP Table Details

QID:	123817
Category:	Local
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	03/07/2017
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
The list details the arp entries enumerated on the host.

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:

Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

```
Address          HWtype  HWaddress          Flags Mask            Iface
172.31.12.49     ether   0a:89:b8:d1:ee:00  C                     eth0
172.18.0.2       ether   02:42:ac:12:00:02  C                     br-ede829f66747
172.31.0.1       ether   0a:96:5b:f1:2f:14  C                     eth0
172.31.0.2       ether   0a:96:5b:f1:2f:14  C                     eth0
```

1 Routing Table Details

QID:	123818
Category:	Local
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	07/06/2018
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
The list details the information about your network topology enumerated from the host.

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

```
Kernel IP routing table
Destination     Gateway         Genmask         Flags Metric Ref    Use Iface
0.0.0.0         172.31.0.1      0.0.0.0         UG    0      0        0 eth0
172.17.0.0      0.0.0.0         255.255.0.0     U     0      0        0 docker0
172.18.0.0      0.0.0.0         255.255.0.0     U     0      0        0 br-ede829f66747
172.31.0.0      0.0.0.0         255.255.240.0   U     0      0        0 eth0

default via 172.31.0.1 dev eth0
172.17.0.0/16 dev docker0  proto kernel  scope link  src 172.17.0.1 linkdown
172.18.0.0/16 dev br-ede829f66747  proto kernel  scope link  src 172.18.0.1
172.31.0.0/20 dev eth0  proto kernel  scope link  src 172.31.4.140
```

1 Unix Last Reboot Date and Time

QID:	124145
Category:	Local
CVE ID:	-

Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	08/21/2016
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
System last reboot date and time for Unix.

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

Last Reboot: Mon Aug 20 10:07:20 UTC 2018
System on for last: 1 day

1 Kernel Routing Tables Information

QID:	125000
Category:	Forensics
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	02/22/2005
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
The result section displays the kernel routing tables for the target host.

IMPACT:
N/A

SOLUTION:
Check to be sure that the information reported adheres to your security policy.

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

Kernel IP routing table

Destination	Gateway	Genmask	Flags	MSS	Window	irtt	Iface
0.0.0.0	172.31.0.1	0.0.0.0	UG	0	0	0	eth0
172.17.0.0	0.0.0.0	255.255.0.0	U	0	0	0	docker0
172.18.0.0	0.0.0.0	255.255.0.0	U	0	0	0	br-ede829f66747
172.31.0.0	0.0.0.0	255.255.240.0	U	0	0	0	eth0

1 Host File Information

QID:	125004
Category:	Forensics
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	08/08/2005
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

The /etc/hosts file is a local database that associates the names of hosts with their Internet Protocol (IP) addresses. The hosts file can be used in conjunction with, or instead of, other hosts databases including the Domain Name System (DNS), the NIS hosts map, and the NIS+ hosts table. Programs use library interfaces to access information in the hosts file.

IMPACT:

The /etc/hosts file can be tampered with in such a way that a hostname is translated into a malicious IP.

SOLUTION:

Make sure that the configuration reported adheres to your security policy.

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

127.0.0.1 localhost

The following lines are desirable for IPv6 capable hosts
::1 ip6-localhost ip6-loopback
fe00::0 ip6-localnet
ff00::0 ip6-mcastprefix
ff02::1 ip6-allnodes
ff02::2 ip6-allrouters
ff02::3 ip6-allhosts

1 Amazon EC2 Linux Instance Metadata

QID:	370098
Category:	Local
CVE ID:	-
Vendor Reference:	Amazon Instance Metadata
Bugtraq ID:	-
Service Modified:	04/06/2018
User Modified:	-
Edited:	No

PCI Vuln: No

THREAT:
Instance metadata is data about your instance that you can use to configure or manage the running instance.

IMPACT:
N/A

SOLUTION:
For more information about metadata please visit Instance Metadata (http://docs.aws.amazon.com/AWSEC2/latest/UserGuide/ec2-instance-metadata.html).

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:
latest/meta-data/ami-id:FAIL:QualysShell not available
latest/meta-data/ami-launch-index:FAIL:QualysShell not available
latest/meta-data/ami-manifest-path:FAIL:QualysShell not available
latest/meta-data/hostname:FAIL:QualysShell not available
latest/meta-data/instance-action:FAIL:QualysShell not available
latest/meta-data/instance-id:FAIL:QualysShell not available
latest/meta-data/instance-type:FAIL:QualysShell not available
latest/meta-data/kernel-id:FAIL:QualysShell not available
latest/meta-data/local-hostname:FAIL:QualysShell not available
latest/meta-data/local-ipv4:FAIL:QualysShell not available
latest/meta-data/mac:FAIL:QualysShell not available
latest/meta-data/public-hostname:FAIL:QualysShell not available
latest/meta-data/public-ipv4:FAIL:QualysShell not available
latest/meta-data/reservation-id:FAIL:QualysShell not available
latest/meta-data/security-groups:FAIL:QualysShell not available
latest/meta-data/ancestor-ami-ids:FAIL:QualysShell not available
latest/meta-data/profile:FAIL:QualysShell not available
latest/dynamic/instance-identity/document/accountId:FAIL:QualysShell not available
latest/dynamic/instance-identity/document/pendingTime:FAIL:QualysShell not available
latest/dynamic/instance-identity/document/version:FAIL:QualysShell not available
latest/dynamic/instance-identity/document/imageId:FAIL:QualysShell not available
latest/dynamic/instance-identity/document/region:FAIL:QualysShell not available
latest/dynamic/instance-identity/document/availabilityZone:FAIL:QualysShell not available
latest/dynamic/instance-identity/document/kernelId:FAIL:QualysShell not available
latest/dynamic/instance-identity/document/instanceId:FAIL:QualysShell not available
latest/dynamic/instance-identity/document/ramdiskId:FAIL:QualysShell not available
latest/dynamic/instance-identity/document/architecture:FAIL:QualysShell not available
latest/dynamic/instance-identity/document/instanceType:FAIL:QualysShell not available
latest/dynamic/instance-identity/document/privateIp:FAIL:QualysShell not available
latest/dynamic/instance-identity/document/devpayProductCodes:FAIL:QualysShell not available
latest/dynamic/instance-identity/document/billingProducts:FAIL:QualysShell not available

 1 Default Web Page port 80/tcp

QID: 12230
Category: CGI
CVE ID: -
Vendor Reference: -
Bugtraq ID: -
Service Modified: 06/17/2014
User Modified: -
Edited: No
PCI Vuln: No

THREAT:
The Result section displays the default Web page for the Web server.

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

```
HTTP/1.1 404 Not Found
Server: nginx/1.10.3 (Ubuntu)
Date: Tue, 21 Aug 2018 17:18:48 GMT
Content-Type: text/html
Content-Length: 178
Connection: keep-alive

<html>
<head><title>404 Not Found</title></head>
<body bgcolor="white">
<center><h1>404 Not Found</h1></center>
<hr><center>nginx/1.10.3 (Ubuntu)</center>
</body>
</html>
```

1 Web Server Version — port 80/tcp

QID:	86000
Category:	Web server
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	10/25/2016
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
N/A

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

Server Version	Server Banner
nginx/1.10.3 (Ubuntu)	nginx/1.10.3 (Ubuntu)

1 Web Server Supports HTTP Request Pipelining port 80/tcp

QID:	86565
Category:	Web server
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	02/22/2005
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
Version 1.1 of the HTTP protocol supports URL-Request Pipelining. This means that instead of using the "Keep-Alive" method to keep the TCP connection alive over multiple requests, the protocol allows multiple HTTP URL requests to be made in the same TCP packet. Any Web server which is HTTP 1.1 compliant should then process all the URLs requested in the single TCP packet and respond as usual.
The target Web server was found to support this functionality of the HTTP 1.1 protocol.

IMPACT:
Support for URL-Request Pipelining has interesting consequences. For example, as explained in this paper by Daniel Roelker (http://www.defcon.org/images/defcon-11/dc-11-presentations/dc-11-Roelker/dc-11-roelker-paper.pdf), it can be used for evading detection by Intrusion Detection Systems. Also, it can be used in HTTP Response-Spliting style attacks.

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:
GET / HTTP/1.1
Host:18.214.224.66:80

GET /Q_Evasive/ HTTP/1.1
Host:18.214.224.66:80

HTTP/1.1 404 Not Found
Server: nginx/1.10.3 (Ubuntu)
Date: Tue, 21 Aug 2018 17:20:13 GMT
Content-Type: text/html
Content-Length: 178
Connection: keep-alive

<html>
<head><title>404 Not Found</title></head>
<body bgcolor="white">
<h1>404 Not Found</h1>
<hr> nginx/1.10.3 (Ubuntu)

</body>
</html>
HTTP/1.1 404 Not Found
Server: nginx/1.10.3 (Ubuntu)
Date: Tue, 21 Aug 2018 17:20:13 GMT
Content-Type: text/html
Content-Length: 178
Connection: keep-alive

<html>
<head><title>404 Not Found</title></head>
<body bgcolor="white">
<h1>404 Not Found</h1>
<hr> nginx/1.10.3 (Ubuntu)
</body>
</html>

1 Default Web Page port 443/tcp over SSL

QID:	12230
Category:	CGI
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	06/17/2014
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
The Result section displays the default Web page for the Web server.

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:
HTTP/1.1 200 OK
Server: nginx/1.10.3 (Ubuntu)
Date: Tue, 21 Aug 2018 17:20:29 GMT
Content-Type: text/html
Content-Length: 0
Connection: keep-alive
Last-Modified: Tue, 01 May 2018 11:34:44 GMT
ETag: "0-56b235b56dd00"
Accept-Ranges: bytes
Strict-Transport-Security: max-age=31536000; includeSubDomains

1 SSL Server Information Retrieval port 443/tcp over SSL

QID:	38116
Category:	General remote services
CVE ID:	-
Vendor Reference:	-

Bugtraq ID: -
Service Modified: 05/24/2016
User Modified: -
Edited: No
PCI Vuln: No

THREAT:

The following is a list of supported SSL ciphers.
Note: If a cipher is included in this list it means that it was possible to establish a SSL connection using that cipher. There are some web servers setups that allow connections to be established using a LOW grade cipher, only to provide a web page stating that the URL is accessible only through a non-LOW grade cipher. In this case even though LOW grade cipher will be listed here QID 38140 will not be reported.

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

CIPHER	KEY-EXCHANGE	AUTHENTICATION	MAC	ENCRYPTION(KEY-STRENGTH)	GRADE
SSLv2 PROTOCOL IS DISABLED					
SSLv3 PROTOCOL IS DISABLED					
TLSv1 PROTOCOL IS ENABLED					
TLSv1	COMPRESSION METHOD	None			
DES-CBC3-SHA	RSA	RSA	SHA1	3DES(168)	MEDIUM
EDH-RSA-DES-CBC3-SHA	DH	RSA	SHA1	3DES(168)	MEDIUM
AES128-SHA	RSA	RSA	SHA1	AES(128)	MEDIUM
DHE-RSA-AES128-SHA	DH	RSA	SHA1	AES(128)	MEDIUM
AES256-SHA	RSA	RSA	SHA1	AES(256)	HIGH
DHE-RSA-AES256-SHA	DH	RSA	SHA1	AES(256)	HIGH
ECDHE-RSA-DES-CBC3-SHA	ECDH	RSA	SHA1	3DES(168)	MEDIUM
ECDHE-RSA-AES128-SHA	ECDH	RSA	SHA1	AES(128)	MEDIUM
ECDHE-RSA-AES256-SHA	ECDH	RSA	SHA1	AES(256)	HIGH
TLSv1.1 PROTOCOL IS ENABLED					
TLSv1.1	COMPRESSION METHOD	None			
DES-CBC3-SHA	RSA	RSA	SHA1	3DES(168)	MEDIUM
EDH-RSA-DES-CBC3-SHA	DH	RSA	SHA1	3DES(168)	MEDIUM
AES128-SHA	RSA	RSA	SHA1	AES(128)	MEDIUM
DHE-RSA-AES128-SHA	DH	RSA	SHA1	AES(128)	MEDIUM
AES256-SHA	RSA	RSA	SHA1	AES(256)	HIGH
DHE-RSA-AES256-SHA	DH	RSA	SHA1	AES(256)	HIGH
ECDHE-RSA-DES-CBC3-SHA	ECDH	RSA	SHA1	3DES(168)	MEDIUM
ECDHE-RSA-AES128-SHA	ECDH	RSA	SHA1	AES(128)	MEDIUM
ECDHE-RSA-AES256-SHA	ECDH	RSA	SHA1	AES(256)	HIGH
TLSv1.2 PROTOCOL IS ENABLED					
TLSv1.2	COMPRESSION METHOD	None			
DES-CBC3-SHA	RSA	RSA	SHA1	3DES(168)	MEDIUM

EDH-RSA-DES-CBC3-SHA	DH	RSA	SHA1	3DES(168)	MEDIUM
AES128-SHA	RSA	RSA	SHA1	AES(128)	MEDIUM
DHE-RSA-AES128-SHA	DH	RSA	SHA1	AES(128)	MEDIUM
AES256-SHA	RSA	RSA	SHA1	AES(256)	HIGH
DHE-RSA-AES256-SHA	DH	RSA	SHA1	AES(256)	HIGH
DHE-RSA-AES128-SHA256	DH	RSA	SHA256	AES(128)	MEDIUM
DHE-RSA-AES256-SHA256	DH	RSA	SHA256	AES(256)	HIGH
AES128-GCM-SHA256	RSA	RSA	AEAD	AESGCM(128)	MEDIUM
AES256-GCM-SHA384	RSA	RSA	AEAD	AESGCM(256)	HIGH
DHE-RSA-AES128-GCM-SHA256	DH	RSA	AEAD	AESGCM(128)	MEDIUM
DHE-RSA-AES256-GCM-SHA384	DH	RSA	AEAD	AESGCM(256)	HIGH
ECDHE-RSA-DES-CBC3-SHA	ECDH	RSA	SHA1	3DES(168)	MEDIUM
ECDHE-RSA-AES128-SHA	ECDH	RSA	SHA1	AES(128)	MEDIUM
ECDHE-RSA-AES256-SHA	ECDH	RSA	SHA1	AES(256)	HIGH
ECDHE-RSA-AES128-SHA256	ECDH	RSA	SHA256	AES(128)	MEDIUM
ECDHE-RSA-AES256-SHA384	ECDH	RSA	SHA384	AES(256)	HIGH
ECDHE-RSA-AES128-GCM-SHA256	ECDH	RSA	AEAD	AESGCM(128)	MEDIUM
ECDHE-RSA-AES256-GCM-SHA384	ECDH	RSA	AEAD	AESGCM(256)	HIGH
AES128-SHA256	RSA	RSA	SHA256	AES(128)	MEDIUM
AES256-SHA256	RSA	RSA	SHA256	AES(256)	HIGH

1 SSL Session Caching Information

port 443/tcp over SSL

QID:	38291
Category:	General remote services
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	09/16/2004
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:

SSL session is a collection of security parameters that are negotiated by the SSL client and server for each SSL connection. SSL session caching is targeted to reduce the overhead of negotiations in recurring SSL connections. SSL sessions can be reused to resume an earlier connection or to establish multiple simultaneous connections. The client suggests an SSL session to be reused by identifying the session with a Session-ID during SSL handshake. If the server finds it appropriate to reuse the session, then they both proceed to secure communication with already known security parameters.
This test determines if SSL session caching is enabled on the host.

IMPACT:

SSL session caching is part of the SSL and TLS protocols and is not a security threat. The result of this test is for informational purposes only.

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

TLSv1 session caching is enabled on the target.
TLSv1.1 session caching is enabled on the target.
TLSv1.2 session caching is enabled on the target.

1 SSL/TLS invalid protocol version tolerance port 443/tcp over SSL

QID:	38597
Category:	General remote services
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	01/29/2016
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
SSL/TLS protocols have different version that can be supported by both the client and the server. This test attempts to send invalid protocol versions to the target in order to find out what is the target's behavior. The results section contains a table that indicates what was the target's response to each of our tests.

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

my version	target version
0304	0303
0399	0303
0400	0303
0499	0303

1 SSL Certificate will expire within next six months port 443/tcp over SSL

QID:	38600
Category:	General remote services
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	01/29/2016
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
Certificates are used for authentication purposes in different protocols such as SSL/TLS. Each certificate has a validity period outside of which it is supposed to be considered invalid. This QID is reported to inform that a certificate will expire within next six months. The advance notice can be helpful since obtaining a certificate can take some time.

IMPACT:
Expired certificates can cause connection disruptions or compromise the integrity and privacy of the connections being protected by the

certificates.

SOLUTION:
Contact the certificate authority that signed your certificate to arrange for a renewal.

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:
Certificate #0 CN=<anon>.area9learning.com The certificate will expire within six months: Nov 18 13:25:09 2018 GMT

1 SSL Server default Diffie-Hellman prime information port 443/tcp over SSL

QID:	38609
Category:	General remote services
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	05/26/2015
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
Diffie-Hellman is a popular cryptographic algorithm used by SSL/TLS.
- For fixed primes: 1024 and below are considered unsafe.

- For variable
primes: 512 is unsafe. 768 is probably mostly safe, but might not be for long. 1024 and above are considered safe.

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:
SSL server default to use Diffie-Hellman key exchange method with variable 2048(bits) prime

1 SSL/TLS Server supports TLS_FALLBACK_SCSV port 443/tcp over SSL

QID:	38610
Category:	General remote services
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-

Service Modified:	06/08/2015
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
TLS cipher suite TLS_FALLBACK_SCSV is a signaling cipher suite value (SCSV).

TLS servers support TLS_FALLBACK_SCSV will prevent downgrade
attack.

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:
TLS_FALLBACK_SCSV is supported on port 443.

1 SSL/TLS Key Exchange Methods — port 443/tcp over SSL

QID:	38704
Category:	General remote services
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	07/12/2018
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
The following is a list of SSL/TLS key exchange methods supported by the server, along with their respective key sizes and strengths.

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

NAME	GROUP	KEY-SIZE	FORWARD-SECRET	CLASSICAL-STRENGTH	QUANTUM-STRENGTH
TLSv1					
RSA		2048	no	110	low
DHE		2048	yes	110	low
ECDHE	secp256r1	256	yes	128	low
TLSv1.1					
RSA		2048	no	110	low
DHE		2048	yes	110	low
ECDHE	secp256r1	256	yes	128	low
TLSv1.2					
RSA		2048	no	110	low
DHE		2048	yes	110	low
ECDHE	secp256r1	256	yes	128	low

1 SSL/TLS Protocol Properties

port 443/tcp over SSL

QID:	38706
Category:	General remote services
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	07/12/2018
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
The following is a list of detected SSL/TLS protocol properties.

IMPACT:
Items include:

Extended Master Secret: indicates whether the extended_master_secret extension is supported or required by the server. This extension enhances security and is recommended. Applicable to TLSv1, TLSv1.1, TLSv1.2, DTLSv1, DTLSv1.2
Encrypt Then MAC: indicates whether the encrypt_then_mac extension is supported or required by the server. This extension enhances the security of non-AEAD ciphers and is recommended. Applicable to TLSv1, TLSv1.1, TLSv1.2, DTLSv1, DTLSv1.2
Heartbeat: indicates whether the heartbeat extension is supported. It is not recommended to enable this, except for DTLS. Applicable to TLSv1, TLSv1.1, TLSv1.2, TLSv1.3, DTLSv1, DTLSv1.2
Truncated HMAC: indicates whether the truncated_hmac extension is supported. This can degrade security and is not recommended. Applicable to TLSv1, TLSv1.1, TLSv1.2, DTLSv1, DTLSv1.2
Cipher priority: indicates whether client, server or both determine the priority of ciphers. Having the server determine the priority is recommended. Applicable to SSLv3, TLSv1, TLSv1.1, TLSv1.2, TLSv1.3, DTLSv1, DTLSv1.2

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

NAME	STATUS

TLSv1	
Extended Master Secret	no
Encrypt Then MAC	no
Heartbeat	yes
Truncated HMAC	no
Cipher priority controlled by	server
TLSv1.1	
Extended Master Secret	no
Encrypt Then MAC	no
Heartbeat	yes
Truncated HMAC	no
Cipher priority controlled by	server
TLSv1.2	
Extended Master Secret	no
Encrypt Then MAC	no
Heartbeat	yes
Truncated HMAC	no
Cipher priority controlled by	server

 1 TLS Secure Renegotiation Extension Support Information port 443/tcp over SSL

QID:	42350
Category:	General remote services
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	03/21/2016
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
Secure Socket Layer (SSL) and Transport Layer Security (TLS) renegotiation are vulnerable to an attack in which the attacker forms a TLS connection with the target server, injects content of his choice, and then splices in a new TLS connection from a client. The server treats the client's initial TLS handshake as a renegotiation and thus believes that the initial data transmitted by the attacker is from the same entity as the subsequent client data. TLS protocol was extended to cryptographically tierenegotiations to the TLS connections they are being performed over. This is referred to as TLS secure renegotiation extension. This detection determines whether the TLS secure renegotiation extension is supported by the server or not.

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:
TLS Secure Renegotiation Extension Status: supported.

QID:	86002
Category:	Web server
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	01/23/2003
User Modified:	-
Edited:	No
PCI Vuln:	No

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

NAME	VALUE
(0)CERTIFICATE 0	
(0)Version	3 (0x2)
(0)Serial Number	03:ca:32:88:ef:93:d0:19:a0:69:f4:56:49:1d:25:84:eb:70
(0)Signature Algorithm	sha256WithRSAEncryption
(0)ISSUER NAME	
countryName	US
organizationName	Let's Encrypt
commonName	Let's Encrypt Authority X3
(0)SUBJECT NAME	
commonName	<anon>.area9learning.com
(0)Valid From	Aug 20 13:25:09 2018 GMT
(0)Valid Till	Nov 18 13:25:09 2018 GMT
(0)Public Key Algorithm	rsaEncryption
(0)RSA Public Key	(2048 bit)
(0)	Public-Key: (2048 bit)
(0)	Modulus:
(0)	00:dc:12:9d:27:67:ba:0a:4f:82:45:b9:f4:e5:3a:
(0)	9f:46:4b:62:5b:3f:8a:05:a7:e8:a1:8f:4c:3f:e2:
(0)	00:88:88:38:1c:ae:69:55:64:98:d6:8e:4c:79:66:
(0)	ef:db:7c:99:5d:e8:14:d0:99:9d:8b:d2:ea:74:5e:
(0)	db:8c:62:ba:51:ca:4e:65:54:74:e8:22:58:82:8d:
(0)	64:d1:73:f7:18:e7:92:84:90:41:cb:52:ad:bc:78:
(0)	8c:9d:04:c3:e1:fc:5b:d5:b7:7c:02:3e:ef:1d:60:
(0)	f3:ae:4f:53:87:d7:68:81:11:17:05:b1:06:73:6d:
(0)	ac:da:a1:53:27:7e:73:1b:85:43:aa:bb:24:c0:33:
(0)	d4:96:4d:01:09:ce:da:00:3c:60:70:ef:de:ae:ff:
(0)	f1:bf:0f:27:62:8b:05:f2:42:78:9c:88:a1:83:0a:
(0)	a1:62:38:08:e6:59:df:78:7b:8c:58:10:b8:06:15:
(0)	7d:8b:9e:53:30:e1:c0:38:db:a8:58:35:60:db:57:
(0)	dc:97:fa:6b:77:50:e6:53:5a:59:09:15:4a:ec:e5:
(0)	0c:f6:d6:8d:3f:54:dc:0b:ab:a0:7d:cf:2c:51:54:
(0)	36:4b:5c:af:76:71:d7:43:79:0b:d4:3b:2d:39:4e:
(0)	7f:07:a9:d7:c7:92:76:ce:cf:de:e8:af:9b:0b:75:

(0)	9d:13
(0)	Exponent: 65537 (0x10001)
(0)X509v3 EXTENSIONS	
(0)X509v3 Key Usage	critical
(0)	Digital Signature, Key Encipherment
(0)X509v3 Extended Key Usage	TLS Web Server Authentication, TLS Web Client Authentication
(0)X509v3 Basic Constraints	critical
(0)	CA:FALSE
(0)X509v3 Subject Key Identifier	D6:C6:6C:D0:11:3D:52:FD:44:54:3A:20:30:95:74:7C:D7:70:A3:8F
(0)X509v3 Authority Key Identifier	keyid:A8:4A:6A:63:04:7D:DD:BA:E6:D1:39:B7:A6:45:65:EF:F3:A8:EC:A1
(0)Authority Information Access	OCSP - URI:http://ocsp.int-x3.letsencrypt.org
(0)	CA Issuers - URI:http://cert.int-x3.letsencrypt.org/
(0)X509v3 Subject Alternative Name	DNS:area9learning.com
(0)X509v3 Certificate Policies	Policy: 2.23.140.1.2.1
(0)	Policy: 1.3.6.1.4.1.44947.1.1.1
(0)	CPS: http://cps.letsencrypt.org
(0)	User Notice:
(0)	Explicit Text: This Certificate may only be relied upon by Relying Parties and only in accordance with the Certificate Policy found at https://letsencrypt.org/repository/
(0)CT Precertificate SCTs	Signed Certificate Timestamp:
(0)	Version : v1(0)
(0)	Log ID : 55:81:D4:C2:16:90:36:01:4A:EA:0B:9B:57:3C:53:F0:
(0)	C0:E4:38:78:70:25:08:17:2F:A3:AA:1D:07:13:D3:0C
(0)	Timestamp : Aug 20 14:25:09.445 2018 GMT
(0)	Extensions: none
(0)	Signature : ecdsa-with-SHA256
(0)	30:44:02:20:41:C8:1B:50:7B:0C:53:12:07:90:17:36:
(0)	77:86:46:C2:44:42:B5:8D:73:8F:55:7A:BE:4E:CB:C2:
(0)	C0:58:A5:D1:02:20:79:E5:91:4B:53:A3:E1:BE:DC:1A:
(0)	31:A8:3E:D2:AA:CC:4A:53:16:F0:8E:02:A9:B6:F3:E3:
(0)	BB:C3:88:A9:93:A3
(0)	Signed Certificate Timestamp:
(0)	Version : v1(0)
(0)	Log ID : 29:3C:51:96:54:C8:39:65:BA:AA:50:FC:58:07:D4:B7:
(0)	6F:BF:58:7A:29:72:DC:A4:C3:0C:F4:E5:45:47:F4:78
(0)	Timestamp : Aug 20 14:25:09.718 2018 GMT
(0)	Extensions: none
(0)	Signature : ecdsa-with-SHA256
(0)	30:46:02:21:00:D2:4C:C4:9E:34:68:87:66:08:63:FC:
(0)	4A:F5:B6:6E:38:55:E2:DD:50:13:36:EA:23:5A:BB:45:
(0)	12:EC:25:29:BA:02:21:00:F3:34:13:72:0D:E7:9C:0E:
(0)	BC:9B:70:50:03:F2:7F:42:B6:A0:74:F0:8B:EC:F6:48:
(0)	6B:67:85:80:7E:E7:84:66
(0)Signature	(256 octets)
(0)	42:a1:89:71:fe:5a:64:d2:71:37:0f:ec:16:4b:3c:08
(0)	2c:a5:b1:10:bc:ac:06:60:b2:20:2d:ef:2c:e5:7a:27
(0)	94:a2:a1:c6:09:ec:92:19:db:56:86:d9:67:d2:8e:83
(0)	3a:df:2d:6e:05:30:c7:c7:02:61:7a:3f:d2:ac:36:5c
(0)	85:c4:54:3d:96:4f:e9:77:a9:79:ca:f9:ca:b5:33:92
(0)	7f:ac:3e:95:d6:bc:9d:af:ea:d1:fc:e8:ff:e0:88:38
(0)	2b:2b:1a:d0:8a:9a:f8:1e:fb:1c:61:e7:cb:75:6e:89
(0)	0c:3c:f4:40:ab:56:48:50:44:98:b1:57:e3:fd:f4:36
(0)	08:f9:f1:ea:3e:8f:95:b1:b6:35:38:56:3c:ce:fb:f3
(0)	d5:82:7f:34:39:21:a3:e0:d6:70:67:d3:f7:e6:2a:c4
(0)	e5:3c:8f:70:b4:ef:27:f5:14:cf:d4:03:b5:25:1d:94

(0)	7e:b8:0d:ef:3b:e2:a6:e2:e1:a7:64:0a:a9:76:1f:d6
(0)	6a:52:ea:74:0e:9c:c0:85:be:44:3e:77:bd:44:16:56
(0)	37:47:ab:cc:5e:6c:7d:55:55:c7:22:45:8b:20:00:b3
(0)	d1:86:1d:98:af:d2:f9:62:72:9d:97:c9:e9:9c:6d:ab
(0)	89:66:27:a3:fe:82:0e:4b:1b:ba:b8:2d:09:28:cc:bf
(1)CERTIFICATE 1	
(1)Version	3 (0x2)
(1)Serial Number	0a:01:41:42:00:00:01:53:85:73:6a:0b:85:ec:a7:08
(1)Signature Algorithm	sha256WithRSAEncryption
(1)ISSUER NAME	
organizationName	Digital Signature Trust Co.
commonName	DST Root CA X3
(1)SUBJECT NAME	
countryName	US
organizationName	Let's Encrypt
commonName	Let's Encrypt Authority X3
(1)Valid From	Mar 17 16:40:46 2016 GMT
(1)Valid Till	Mar 17 16:40:46 2021 GMT
(1)Public Key Algorithm	rsaEncryption
(1)RSA Public Key	(2048 bit)
(1)	Public-Key: (2048 bit)
(1)	Modulus:
(1)	00:9c:d3:0c:f0:5a:e5:2e:47:b7:72:5d:37:83:b3:
(1)	68:63:30:ea:d7:35:26:19:25:e1:bd:be:35:f1:70:
(1)	92:2f:b7:b8:4b:41:05:ab:a9:9e:35:08:58:ec:b1:
(1)	2a:c4:68:87:0b:a3:e3:75:e4:e6:f3:a7:62:71:ba:
(1)	79:81:60:1f:d7:91:9a:9f:f3:d0:78:67:71:c8:69:
(1)	0e:95:91:cf:fe:e6:99:e9:60:3c:48:cc:7e:ca:4d:
(1)	77:12:24:9d:47:1b:5a:eb:b9:ec:1e:37:00:1c:9c:
(1)	ac:7b:a7:05:ea:ce:4a:eb:bd:41:e5:36:98:b9:cb:
(1)	fd:6d:3c:96:68:df:23:2a:42:90:0c:86:74:67:c8:
(1)	7f:a5:9a:b8:52:61:14:13:3f:65:e9:82:87:cb:db:
(1)	fa:0e:56:f6:86:89:f3:85:3f:97:86:af:b0:dc:1a:
(1)	ef:6b:0d:95:16:7d:c4:2b:a0:65:b2:99:04:36:75:
(1)	80:6b:ac:4a:f3:1b:90:49:78:2f:a2:96:4f:2a:20:
(1)	25:29:04:c6:74:c0:d0:31:cd:8f:31:38:95:16:ba:
(1)	a8:33:b8:43:f1:b1:1f:c3:30:7f:a2:79:31:13:3d:
(1)	2d:36:f8:e3:fc:f2:33:6a:b9:39:31:c5:af:c4:8d:
(1)	0d:1d:64:16:33:aa:fa:84:29:b6:d4:0b:c0:d8:7d:
(1)	c3:93
(1)	Exponent: 65537 (0x10001)
(1)X509v3 EXTENSIONS	
(1)X509v3 Basic Constraints	critical
(1)	CA:TRUE, pathlen:0
(1)X509v3 Key Usage	critical
(1)	Digital Signature, Certificate Sign, CRL Sign
(1)Authority Information Access	OCSP - URI:http://isrg.trustid.ocsp.identrust.com
(1)	CA Issuers - URI:http://apps.identrust.com/roots/dstrootcax3.p7c
(1)X509v3 Authority Key Identifier	keyid:C4:A7:B1:A4:7B:2C:71:FA:DB:E1:4B:90:75:FF:C4:15:60:85:89:10
(1)X509v3 Certificate Policies	Policy: 2.23.140.1.2.1
(1)	Policy: 1.3.6.1.4.1.44947.1.1.1
(1)	CPS: http://cps.root-x1.letsencrypt.org
(1)X509v3 CRL Distribution Points	
(1)	Full Name:
(1)	URI:http://crl.identrust.com/DSTROOTCAX3CRL.crl

(1)X509v3 Subject Key Identifier	A8:4A:6A:63:04:7D:DD:BA:E6:D1:39:B7:A6:45:65:EF:F3:A8:EC:A1
(1)Signature	(256 octets)
(1)	dd:33:d7:11:f3:63:58:38:dd:18:15:fb:09:55:be:76
(1)	56:b9:70:48:a5:69:47:27:7b:c2:24:08:92:f1:5a:1f
(1)	4a:12:29:37:24:74:51:1c:62:68:b8:cd:95:70:67:e5
(1)	f7:a4:bc:4e:28:51:cd:9b:e8:ae:87:9d:ea:d8:ba:5a
(1)	a1:01:9a:dc:f0:dd:6a:1d:6a:d8:3e:57:23:9e:a6:1e
(1)	04:62:9a:ff:d7:05:ca:b7:1f:3f:c0:0a:48:bc:94:b0
(1)	b6:65:62:e0:c1:54:e5:a3:2a:ad:20:c4:e9:e6:bb:dc
(1)	c8:f6:b5:c3:32:a3:98:cc:77:a8:e6:79:65:07:2b:cb
(1)	28:fe:3a:16:52:81:ce:52:0c:2e:5f:83:e8:d5:06:33
(1)	fb:77:6c:ce:40:ea:32:9e:1f:92:5c:41:c1:74:6c:5b
(1)	5d:0a:5f:33:cc:4d:9f:ac:38:f0:2f:7b:2c:62:9d:d9
(1)	a3:91:6f:25:1b:2f:90:b1:19:46:3d:f6:7e:1b:a6:7a
(1)	87:b9:a3:7a:6d:18:fa:25:a5:91:87:15:e0:f2:16:2f
(1)	58:b0:06:2f:2c:68:26:c6:4b:98:cd:da:9f:0c:f9:7f
(1)	90:ed:43:4a:12:44:4e:6f:73:7a:28:ea:a4:aa:6e:7b
(1)	4c:7d:87:dd:e0:c9:02:44:a7:87:af:c3:34:5b:b4:42

 1 Web Server Supports HTTP Request Pipelining port 443/tcp over SSL

QID:	86565
Category:	Web server
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	02/22/2005
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
Version 1.1 of the HTTP protocol supports URL-Request Pipelining. This means that instead of using the "Keep-Alive" method to keep the TCP connection alive over multiple requests, the protocol allows multiple HTTP URL requests to be made in the same TCP packet. Any Web server which is HTTP 1.1 compliant should then process all the URLs requested in the single TCP packet and respond as usual.
The target Web server was found to support this functionality of the HTTP 1.1 protocol.

IMPACT:
Support for URL-Request Pipelining has interesting consequences. For example, as explained in this paper by Daniel Roelker (http://www.defcon.org/images/defcon-11/dc-11-presentations/dc-11-Roelker/dc-11-roelker-paper.pdf), it can be used for evading detection by Intrusion Detection Systems. Also, it can be used in HTTP Response-Spliting style attacks.

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:
GET / HTTP/1.1
Host:18.214.224.66:443

GET /Q_Evasive/ HTTP/1.1

Host:18.214.224.66:443

HTTP/1.1 200 OK
Server: nginx/1.10.3 (Ubuntu)
Date: Tue, 21 Aug 2018 17:20:10 GMT
Content-Type: text/html
Content-Length: 0
Connection: keep-alive
Last-Modified: Tue, 01 May 2018 11:34:44 GMT
ETag: "0-56b235b56dd00"
Accept-Ranges: bytes
Strict-Transport-Security: max-age=31536000; includeSubDomains

HTTP/1.1 404 Not Found
Server: nginx/1.10.3 (Ubuntu)
Date: Tue, 21 Aug 2018 17:20:10 GMT
Content-Type: text/html; charset=iso-8859-1
Content-Length: 208
Connection: keep-alive

<!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN">
<html><head>
<title>404 Not Found</title>
</head><body>
<h1>Not Found</h1>
The requested URL /Q_Evasive/ was not found on this server.
</body></html>

 1 SSH daemon information retrieving port 22/tcp

QID:	38047
Category:	General remote services
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	04/04/2018
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
SSH is a secure protocol, provided it is fully patched, properly configured, and uses FIPS approved algorithms.

For Red Hat ES 4:-
SSH1 supported yes
Supported authentification methods for SSH1 RSA,password
Supported ciphers for SSH1 3des,blowfish
SSH2 supported yes
Supported keys exchange algorithm for SSH2 diffie-hellman-group-exchange-sha1,diffie-hellman-group14-sha1,diffie-hellman-group1-sha1
Supported decryption ciphers for SSH2 aes128-cbc,3des-cbc,blowfish-cbc,cast128-cbc,arcfour,aes192-cbc,aes256-cbc,rijndael-cbc@lysator.liu.se,aes128-ctr,aes192-ctr,aes256-ctr
Supported encryption ciphers for SSH2 aes128-cbc,3des-cbc,blowfish-cbc,cast128-cbc,arcfour,aes192-cbc,aes256-cbc,rijndael-cbc@lysator.liu.se,aes128-ctr,aes192-ctr,aes256-ctr
Supported decryption mac for SSH2 hmac-md5,hmac-sha1,hmac-ripemd160,hmac-ripemd160@openssh.com,hmac-sha1-96,hmac-md5-96
Supported encryption mac for SSH2 hmac-md5,hmac-sha1,hmac-ripemd160,hmac-ripemd160@openssh.com,hmac-sha1-96,hmac-md5-96
Supported authentification methods for SSH2 publickey,gssapi-with-mic,password

IMPACT:
Successful exploitation allows an attacker to execute arbitrary commands on the SSH server or otherwise subvert an encrypted SSH channel with arbitrary data.

SOLUTION:
SSH version 2 is preferred over SSH version 1.

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

SSH1 supported	no
SSH2 supported	yes
Supported key exchange algorithms for SSH2	curve25519-sha256@libssh.org, ecdh-sha2-nistp256, ecdh-sha2-nistp384, ecdh-sha2-nistp521, diffie-hellman-group-exchange-sha256, diffie-hellman-group14-sha1
Supported host key algorithms for SSH2	ssh-rsa, rsa-sha2-512, rsa-sha2-256, ecdsa-sha2-nistp256, ssh-ed25519
Supported decryption ciphers for SSH2	chacha20-poly1305@openssh.com, aes128-ctr, aes192-ctr, aes256-ctr, aes128-gcm@openssh.com, aes256-gcm@openssh.com
Supported encryption ciphers for SSH2	chacha20-poly1305@openssh.com, aes128-ctr, aes192-ctr, aes256-ctr, aes128-gcm@openssh.com, aes256-gcm@openssh.com
Supported decryption macs for SSH2	umac-64-etm@openssh.com, umac-128-etm@openssh.com, hmac-sha2-256-etm@openssh.com, hmac-sha2-512-etm@openssh.com, hmac-sha1-etm@openssh.com, umac-64@openssh.com, umac-128@openssh.com, hmac-sha2-256, hmac-sha2-512, hmac-sha1
Supported encryption macs for SSH2	umac-64-etm@openssh.com, umac-128-etm@openssh.com, hmac-sha2-256-etm@openssh.com, hmac-sha2-512-etm@openssh.com, hmac-sha1-etm@openssh.com, umac-64@openssh.com, umac-128@openssh.com, hmac-sha2-256, hmac-sha2-512, hmac-sha1
Supported decompression for SSH2	none, zlib@openssh.com
Supported compression for SSH2	none, zlib@openssh.com
Supported authentication methods for SSH2	publickey

 1 SSH Banner port 22/tcp

QID: 38050
Category: General remote services
CVE ID: -
Vendor Reference: -
Bugtraq ID: -
Service Modified: 02/04/2003
User Modified: -
Edited: No
PCI Vuln: No

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:
SSH-2.0-OpenSSH_7.2p2 Ubuntu-4ubuntu2.4

 1 Unix Authentication Method port 22/tcp

QID: 38307
Category: General remote services
CVE ID: -
Vendor Reference: -
Bugtraq ID: -

Service Modified:	09/06/2005
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
Unix authentication was performed. The Result section in your detailed results displays the authentication method that was used for this host. Unix authentication is used to obtain remote access to different command line services such as SSH, telnet and rlogin. Specified credentials must include a user name and may include a password, an RSA private key and/or a DSA private key. When authenticating to target hosts that support SSH2, authentication is attempted in the following order: 1) RSA key, 2) DSA key and 3) user name and password. For target hosts that only support SSH1, only the supplied user name and password are used for authentication.

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

User Name	svc-qlys
Authentication Scheme	publickey(Key #1: RSA key)
Protocol	SSH Version 2
Discovery Method	Login credentials provided by user
Using sudo	No
Key exchange algorithm	curve25519-sha256@libssh.org
Host key algorithm	ssh-ed25519
Compression algorithm	zlib@openssh.com
Encryption algorithm	chacha20-poly1305@openssh.com
MAC algorithm	AEAD
Key #1 MD5 key fingerprint	MD5:b1:c4:52:a8:c8:75:19:5b:2e:cd:7d:5c:69:33:19:31
Key #1 SHA256 key fingerprint	SHA256:Bpy/y1jJ9IuIVL7nuSTn9hOUSzI/uZbIqS7WVIhM02Y=
Authentication Record	Linux Credentials

1 SSHD (SSH Daemon) PermitRootLogin Configuration Setting

port 22/tcp

QID:	38582
Category:	General remote services
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	06/18/2007
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
SSHD (SSH Daemon) reads configuration data from the sshd_config file.

The PermitRootLogin entry specifies whether root can log in using SSH. The default setting is " PermitRootLogin yes" for most systems.

IMPACT:
If the PermitRootLogin is set to yes, root is able to login through SSH.

SOLUTION:
Only allow root if absolutely necessary.
To disable remote root login via SSH, edit the sshd_config file and change the line:

PermitRootLogin yes

To:

PermitRootLogin no

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:
-rw-r--r-- 1 root root 2540 Jun 27 08:28 /etc/ssh/sshd_config

PermitRootLogin prohibit-password
--
the setting of "PermitRootLogin without-password".

 1 Default Web Page port 8080/tcp

QID:	12230
Category:	CGI
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	06/17/2014
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
The Result section displays the default Web page for the Web server.

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:
HTTP/1.1 200 OK

Date: Tue, 21 Aug 2018 17:19:57 GMT
Server: Apache
Last-Modified: Tue, 01 May 2018 11:34:44 GMT
ETag: "0-56b235b56dd00"
Accept-Ranges: bytes
Content-Length: 0
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive
Content-Type: text/html

1 HTTP Methods Returned by OPTIONS Request port 8080/tcp

QID:	45056
Category:	Information gathering
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	01/16/2006
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
The HTTP methods returned in response to an OPTIONS request to the Web server detected on the target host are listed.

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:
Allow: OPTIONS,GET,HEAD,POST

1 Web Server Version port 8080/tcp

QID:	86000
Category:	Web server
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	10/25/2016
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
N/A

IMPACT:

N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

Server Version	Server Banner
Apache	Apache

1 Apache Web Server Detected port 8080/tcp

QID:	86496
Category:	Web server
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	10/03/2016
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
Apache, the open source web server software that is developed and maintained by Apache Software Foundation is detected on the host.

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:
Apache web server detected on port 8080 - Apache

1 Web Server Supports HTTP Request Pipelining port 8080/tcp

QID:	86565
Category:	Web server
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	02/22/2005

User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
Version 1.1 of the HTTP protocol supports URL-Request Pipelining. This means that instead of using the "Keep-Alive" method to keep the TCP connection alive over multiple requests, the protocol allows multiple HTTP URL requests to be made in the same TCP packet. Any Web server which is HTTP 1.1 compliant should then process all the URLs requested in the single TCP packet and respond as usual.
The target Web server was found to support this functionality of the HTTP 1.1 protocol.

IMPACT:
Support for URL-Request Pipelining has interesting consequences. For example, as explained in this paper by Daniel Roelker (http://www.defcon.org/images/defcon-11/dc-11-presentations/dc-11-Roelker/dc-11-roelker-paper.pdf), it can be used for evading detection by Intrusion Detection Systems. Also, it can be used in HTTP Response-Spliting style attacks.

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

```
GET / HTTP/1.1
Host:18.214.224.66:8080

GET /Q_Evasive/ HTTP/1.1
Host:18.214.224.66:8080



HTTP/1.1 200 OK
Date: Tue, 21 Aug 2018 17:20:16 GMT
Server: Apache
Last-Modified: Tue, 01 May 2018 11:34:44 GMT
ETag: "0-56b235b56dd00"
Accept-Ranges: bytes
Content-Length: 0
Content-Type: text/html

HTTP/1.1 404 Not Found
Date: Tue, 21 Aug 2018 17:20:16 GMT
Server: Apache
Content-Length: 208
Content-Type: text/html; charset=iso-8859-1

<!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN">
<html><head>
<title>404 Not Found</title>
</head><body>
<h1>Not Found</h1>
<p>The requested URL /Q_Evasive/ was not found on this server.</p>
</body></html>
```

1 HTTP Methods Returned by OPTIONS Request — port 443/tcp

QID:	45056
Category:	Information gathering
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-

Service Modified: 01/16/2006
User Modified: -
Edited: No
PCI Vuln: No

THREAT:
The HTTP methods returned in response to an OPTIONS request to the Web server detected on the target host are listed.

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:
Allow: OPTIONS,GET,HEAD,POST

1 SSL Web Server Version port 443/tcp

QID: 86001
Category: Web server
CVE ID: -
Vendor Reference: -
Bugtraq ID: -
Service Modified: 01/01/1999
User Modified: -
Edited: No
PCI Vuln: No

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:

Server Version	Server Banner
nginx/1.10.3 (Ubuntu)	nginx/1.10.3 (Ubuntu)

1 HTTP Strict Transport Security (HSTS) Support Detected port 443/tcp

QID: 86137
Category: Web server
CVE ID: -
Vendor Reference: -

Bugtraq ID:	-
Service Modified:	06/08/2015
User Modified:	-
Edited:	No
PCI Vuln:	No

THREAT:
HTTP Strict Transport Security (HSTS) is an opt-in security enhancement that is specified by a web application through the use of a special response header. Once a supported browser receives this header that browser will prevent any communications from being sent over HTTP to the specified domain and will instead send all communications over HTTPS.

IMPACT:
N/A

SOLUTION:
N/A

COMPLIANCE:
Not Applicable

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:
Strict-Transport-Security: max-age=31536000; includeSubDomains

Appendix

Hosts Scanned (IP)

18.214.224.66

Target distribution across scanner appliances

External : 18.214.224.66

Unix/Cisco/Checkpoint Firewall authentication was successful for these hosts (1)

Instance os:
18.214.224.66

Options Profile

SAT Profile - QA/AUT

Scan Settings

Ports:	
Scanned TCP Ports:	Standard Scan
Scanned UDP Ports:	Light Scan
Scan Dead Hosts:	Off
Load Balancer Detection:	Off
Perform 3-way Handshake:	Off
Authoritative Option:	Off
Vulnerability Detection:	Complete
Include OVAL Checks:	yes
Password Brute Forcing:	
System:	Disabled
Custom:	Disabled
Authentication:	
Windows:	Enabled
Unix/Cisco:	Enabled
Oracle:	Enabled
Oracle Listener:	Disabled
SNMP:	Disabled
VMware:	Disabled
DB2:	Disabled
HTTP:	Disabled
MySQL:	Disabled
Tomcat Server:	Disabled
MongoDB:	Disabled
Palo Alto Networks Firewall:	Disabled
Overall Performance:	Custom
Authenticated Scan Certificate Discovery:	Disabled
Test Authentication:	Disabled
Hosts to Scan in Parallel:	
Use Appliance Parallel ML Scaling:	Off
External Scanners:	17
Scanner Appliances:	30
Processes to Run in Parallel:	

Total Processes:	10
HTTP Processes:	10
Packet (Burst) Delay:	Medium
Port Scanning and Host Discovery:	
Intensity:	Normal
Dissolvable Agent:	
Dissolvable Agent (for this profile):	Disabled
Windows Share Enumeration:	Disabled
Windows Directory Search:	Disabled
Lite OS Discovery:	Disabled
Host Alive Testing:	Disabled
Do Not Overwrite OS:	Disabled

Advanced Settings

Host Discovery:	TCP Standard Scan, UDP None, ICMP On
Ignore firewall-generated TCP RST packets:	On
Ignore all TCP RST packets:	Off
Ignore firewall-generated TCP SYN-ACK packets:	On
Do not send TCP ACK or SYN-ACK packets during host discovery:	On

Report Legend

Vulnerability Levels

A Vulnerability is a design flaw or mis-configuration which makes your network (or a host on your network) susceptible to malicious attacks from local or remote users. Vulnerabilities can exist in several areas of your network, such as in your firewalls, FTP servers, Web servers, operating systems or CGI bins. Depending on the level of the security risk, the successful exploitation of a vulnerability can vary from the disclosure of information about the host to a complete compromise of the host.

Severity	Level	Description
1	Minimal	Intruders can collect information about the host (open ports, services, etc.) and may be able to use this information to find other vulnerabilities.
2	Medium	Intruders may be able to collect sensitive information from the host, such as the precise version of software installed. With this information, intruders can easily exploit known vulnerabilities specific to software versions.
3	Serious	Intruders may be able to gain access to specific information stored on the host, including security settings. This could result in potential misuse of the host by intruders. For example, vulnerabilities at this level may include partial disclosure of file contents, access to certain files on the host, directory browsing, disclosure of filtering rules and security mechanisms, denial of service attacks, and unauthorized use of services, such as mail-relaying.
4	Critical	Intruders can possibly gain control of the host, or there may be potential leakage of highly sensitive information. For example, vulnerabilities at this level may include full read access to files, potential backdoors, or a listing of all the users on the host.
5	Urgent	Intruders can easily gain control of the host, which can lead to the compromise of your entire network security. For example, vulnerabilities at this level may include full read and write access to files, remote execution of commands, and the presence of backdoors.

Potential Vulnerability Levels

A potential vulnerability is one which we cannot confirm exists. The only way to verify the existence of such vulnerabilities on your network would be to perform an intrusive scan, which could result in a denial of service. This is strictly against our policy. Instead, we urge you to investigate these potential vulnerabilities further.

Severity	Level	Description
1	Minimal	If this vulnerability exists on your system, intruders can collect information about the host (open ports, services, etc.) and may be able to use this information to find other vulnerabilities.
2	Medium	If this vulnerability exists on your system, intruders may be able to collect sensitive information from the host, such as the precise version of software installed. With this information, intruders can easily exploit known vulnerabilities specific to software versions.
3	Serious	If this vulnerability exists on your system, intruders may be able to gain access to specific information stored on the host, including security settings. This could result in potential misuse of the host by intruders. For example, vulnerabilities at this level may include partial disclosure of file contents, access to certain files on the host, directory browsing, disclosure of

Severity	Level	Description
		filtering rules and security mechanisms, denial of service attacks, and unauthorized use of services, such as mail-relaying.
4	Critical	If this vulnerability exists on your system, intruders can possibly gain control of the host, or there may be potential leakage of highly sensitive information. For example, vulnerabilities at this level may include full read access to files, potential backdoors, or a listing of all the users on the host.
5	Urgent	If this vulnerability exists on your system, intruders can easily gain control of the host, which can lead to the compromise of your entire network security. For example, vulnerabilities at this level may include full read and write access to files, remote execution of commands, and the presence of backdoors.

Information Gathered

Information Gathered includes visible information about the network related to the host, such as traceroute information, Internet Service Provider (ISP), or a list of reachable hosts. Information Gathered severity levels also include Network Mapping data, such as detected firewalls, SMTP banners, or a list of open TCP services.

Severity	Level	Description
1	Minimal	Intruders may be able to retrieve sensitive information related to the host, such as open UDP and TCP services lists, and detection of firewalls.
2	Medium	Intruders may be able to determine the operating system running on the host, and view banner versions.
3	Serious	Intruders may be able to detect highly sensitive data, such as global system user lists.

Footnotes

This footnote indicates that the CVSS Base score that is displayed for the vulnerability is not supplied by NIST. When the service looked up the latest NIST score for the vulnerability, as published in the National Vulnerability Database (NVD), NIST either listed the CVSS Base score as 0 or did not provide a score in the NVD. In this case, the service determined that the severity of the vulnerability warranted a higher CVSS Base score. The score provided by the service is displayed.