Official Mocana Security Advisory

Advisory Number: #201409A
Advisory Date: April 9, 2014
Advisory Title: Heartbleed OpenSSL Bug

Security Issue:
The Reuters news service and other news sources are reporting that a serious vulnerability exists within OpenSSL's implementation of the TLS/DTLS (transport layer security protocols) heartbeat extension (RFC6520). Exploitation of this may leak memory contents from the web server to the client and from the client to the web server. The flaw was apparently introduced in OpenSSL in December 2011, and has been known to criminal attackers since March 2012. The attacks are stealth and leave no residual traces.

MITRE’s Common Vulnerabilities and Exposures List states "The (1) TLS and (2) DTLS implementations in OpenSSL 1.0.1 before 1.0.1g do not properly handle Heartbeat Extension packets, which allows remote attackers to obtain sensitive information from process memory via crafted packets that trigger a buffer over-read, as demonstrated by reading private keys, related to d1_both.c and t1_lib.c, aka the Heartbleed bug."

Impact
The Heartbleed bug is very serious in that it allows anyone on the Internet who exploits it to read the memory of the systems protected by the vulnerable versions of the OpenSSL software. This vulnerability compromises the secret keys used to identify the service providers and to encrypt the traffic. It exposes the names and passwords of the users as well as the actual content. Thus criminal attackers use this to eavesdrop upon otherwise secure communications and/or steal data from services and users. They may also be able to impersonate services and users.

Mocana Software Affected
Mocana Atlas
Mobile Application Protection (MAP) Console

Mocana Software NOT Affected
NanoSSL
KeyVPN

How to Determine if You’re Affected
To be safe, you should perform a source code review of your applications. You should make sure that if you do use OpenSSL the heartbeat routines/calls have NOT been activated.

Status of different OpenSSL versions:

- OpenSSL 1.0.1 through 1.0.1f (inclusive) are vulnerable
- OpenSSL 1.0.1g is NOT vulnerable
- OpenSSL 1.0.0 branch is NOT vulnerable
- OpenSSL 0.9.8 branch is NOT vulnerable

Your Options
OpenSSL team has issued a patch: https://www.openssl.org/news/secadv_20140407.txt

The latest patched version 1.0.1g or newer should be used going forward. In cases where it is not possible to patch the software, it is recommended that developers recompile OpenSSL with the handshake removed from the code by using the compile time option -DOPENSSL_NO_HEARTBEATS.
Mocana’s Recommendations
If you do use OpenSSL make sure the heartbeat routines/calls have NOT been activated. At a minimum, new devices and software you roll out should not ship with a version of OpenSSL older than 1.0.1g.

Mocana’s Actions
If you are using Mocana Atlas, OpenSSL is used for CRL checking and web management/interface purposes. CRL checking is not affected by the heartbeat bug. While the web management/interface is an issue, it is only exposed on the internal network and will be fixed in next week's release.

Mocana’s KeyVPN code does not use OpenSSL.
Mocana’s NanoSSL code does not use OpenSSL.

If you are using MAP, the MAP console does use OpenSSL with Apache, however, this can be mitigated by applying the proper OS patch (sudo apt-get update; sudo apt-get dist-upgrade on Ubuntu; or yum update on CentOS).

Further Reading & Resources
2. NIST https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-0160

Disclaimer
The information provided in this Mocana Security Advisory is provided "as is" without warranty of any kind. Mocana disclaims all warranties, either express or implied, including the warranties of merchantability and fitness for a particular purpose. In no event shall Mocana Corporation or its suppliers be liable for any damages whatsoever including direct, indirect, incidental, consequential, loss of business profits or special damages, even if Mocana Corporation or its suppliers have been advised of the possibility of such damages. Some states do not allow the exclusion or limitation of liability for consequential or incidental damages so the foregoing limitation may not apply.

Revisions to this Document; Log Below
Version 1, authored by Robert Vamosi CISSP, Mocana, April 9th 2014.