ActiveVideo Customer Product Notification

Date Issued:	**10/25/2018**
Action Required:	**Yes**
Affected Component:	**PSM – All versions/releases**
Type of Action:	**Configuration Change**
Urgency:	**High, service impact possible**

Description:

ActiveVideo has identified an unpatched flaw in the Aerospike Open Source software that will affect the PSM component. When non-Aerospike data is received on Aerospike heart beat port 3002, the Aerospike service will fail and stop running. This can result in the loss of access to HTML cookie/localstorage data and/or session-based encryption keys.

Recommended Actions:

Aerospike has not provided a full software/code remediation for this issue, only a mitigation. After evaluating the mitigation, ActiveVideo remains concerned that the reliability of Aerospike cannot be guaranteed with the mitigation. Until a full remediation is provided by Aerospike, ActiveVideo is advising all customers to enable the local firewall to block port 3002 from being accessible by any non-PSM components or servers. There is no performance impact by enabling the local firewall.

Please execute the following procedures at your earliest possible convenience.

For ActiveVideo PSM v2.9.x or Lower:

The following process will enable iptables and block all non-PSM servers

1. Login to the first PSM as root or an account with root level access
2. Ensure iptables is set to auto start, is running, and set with empty accept all rules with the following commands:

```
chkconfig on iptables
service iptables start
lokkit --disabled
```

3. Use the following command to add an allow rule for the first PSM server

   NOTE: Replace <PSM-IP> with the IP of *this* PSM server

   ```
   iptables -A INPUT -p tcp --destination-port 3002 -s <PSM-
   IP> -j ACCEPT
   ```

4. Repeat the last step and add a rule for every PSM server in the deployment.

   > **NOTE**: For 3 PSM servers, you would run this command three times, putting in the IP of that PSM server

5. Use the following command to create the rule to block all non-PSM server traffic:

   ```
   iptables -A INPUT -p tcp --destination-port 3002 -j REJECT
   ```

6. Use the following command to commit and save the changes:

   ```
   iptables-save
   ```

7. Verify the changes are present and applied using the following command:

   ```
   iptables -S
   ```

   The output should look like this (in this example, the PSM servers are 10.250.90.30 and 10.250.90.31)

   ```
   -P INPUT ACCEPT
   -P FORWARD ACCEPT
   -P OUTPUT ACCEPT
   -A INPUT -s 10.250.90.30/32 -p tcp -m tcp --dport 3002 -j
   ACCEPT
   -A INPUT -s 10.250.90.31/32 -p tcp -m tcp --dport 3002 -j
   ACCEPT
   -A INPUT -p tcp -m tcp --dport 3002 -j DROP
   ```

8. Repeat these steps for each PSM server

For ActiveVideo PSM v2.10.x and higher:

The following process will enable iptables and block all non-PSM servers

1. Login to the first PSM as root or an account with root level access

2. Ensure firewalld is set to auto start and is running with the following command:

```
systemctl enable --now firewalld
```

3. Use the following command to set the default zone:

```
firewall-cmd --set-default-zone=trusted
```

4. Use the following commands to block traffic to port 3002 by default.

```
firewall-cmd --permanent --zone=trusted --add-rich-
rule='rule family="ipv4" port protocol="tcp" port="3002"
reject'

firewall-cmd --permanent --zone=trusted --add-rich-
rule='rule family="ipv6" port protocol="tcp" port="3002"
reject'
```

5. Using the following commands to create a new firewalld zone and name it for its purpose:

```
firewall-cmd --permanent --new-zone=psmheartbeat
```

6. Using the following command to add port 3002 to be allowed:

```
firewall-cmd --permanent --zone=psmheartbeat --add-
port=3002/tcp
```

7. Use the following command to add a PSM server IP to the allow zone:
   NOTE: Replace <PSM-IP> with the IP of *this* PSM server

```
firewall-cmd --permanent --zone=psmheartbeat --add-
source=<PSM-IP>/32
```

9. Repeat the last step and add a rule for every PSM server in the deployment.

   NOTE: For 3 PSM servers, you would run this command three times, putting in the IP of that PSM server

8. Use the following command to apply all changes:

```
systemctl restart firewalld
```

9. Verify the changes are present and port 3002 is denied by default using the following command:

```
firewall-cmd --list-all
```

The output should look like this (in this example, the PSM servers are 10.250.90.30 and 10.250.90.31)

```
trusted
  target: ACCEPT
  icmp-block-inversion: no
  interfaces:
  sources:
  services:
  ports:
  protocols:
  masquerade: no
  forward-ports:
  source-ports:
  icmp-blocks:
  rich rules:
rule family="ipv6" port port="3002" protocol="tcp" reject
rule family="ipv4" port port="3002" protocol="tcp" reject
```

10. Verify the new zone is defined and the PSM hosts are present using the following command:

```
firewall-cmd --list-all --zone=psmheartbeat
```

The output should look like this (in this example, the PSM servers are 10.250.90.30 and 10.250.90.31)

```
psmheartbeat (active)
  target: default
  icmp-block-inversion: no
  interfaces:
  sources: 10.250.90.30 10.250.90.31
  services:
  ports: 3002/tcp
  protocols:
  masquerade: no
  forward-ports:
  source-ports:
```

```
  icmp-blocks:
  rich rules:
```

11. Repeat these steps for each PSM server

Should you have any further questions or require additional assistance, please reach out to the ActiveVideo Support team at _NOC@activevideo.com or contact your ActiveVideo support representative. Thank you.