TippingPoint Product Bulletin

Product Bulletin #: 1088

Subject: Security Advisory – Update for OpenSSL Vulnerability (CVE-2021-3449)

Date of Announcement: June 4, 2021

Summary: An OpenSSL vulnerability (CVE-2021-3449) exists within TPS 5.3.0, 5.3.1, 5.3.2, 5.4.0, and 5.4.1 TOS versions that can cause the appliance to enter Layer-2 Fallback (L2FB) mode and stop inspecting network traffic.

This vulnerability uses a maliciously crafted message within TLS1.2 renegotiation that causes the TLS Server used by TLS Inspection to halt. This halt forces the appliance to enter L2FB, during which time no traffic will be inspected.

Further details on this vulnerability can be found here:

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-3449

Mitigations: We have removed the vulnerable OpenSSL version and upgraded to the latest non-vulnerable version. This resolution will be included in the next TPS TOS release.

This mitigation can be applied now (before the next TPS TOS release) to remove the ability for renegotiation to occur. The mitigation will block the malicious renegotiation message from being incorrectly interpreted by the appliance; without adversely impacting system performance. This mitigation removes the vulnerability to this CVE.

To apply this mitigation, complete the following steps:

1. Run the following command at the appliance(s) CLI:

   debug ini-cfg modify netpal.ini.handle [SslInsp] npSslNoRenegotiation 1 create

2. Reboot the appliance(s)

If you have concerns or further questions regarding this issue, contact the Trend Micro TippingPoint Technical Assistance Center (TAC).

Thank you,
Trend Micro™ TippingPoint

For contact information, please click here.

.