Silver Peak Security Advisory

Pre-Release Notification

Multiple OpenSSL Vulnerabilities

Buffer underflow with X.509 certificates and man-in-the-middle padding attack vulnerabilities

CVE-2016-2108, CVE-2016-2107 published by OpenSSL on May 3, 2016

Summary:

This is an OpenSSL security advisory for CVE-2016-2108 and CVE-2016-2107 and is dated May 3, 2016.

The issue CVE-2016-2108 affects applications that parse and re-encode X509 certificates. Applications that verify RSA signatures on X509 certificates may also be vulnerable; however, only certificates with valid signatures trigger ASN.1 re-encoding and hence the bug. Specifically, since OpenSSL's default TLS X509 chain verification code verifies the certificate chain from root to leaf, TLS handshakes could only be targeted with valid certificates issued by trusted Certification Authorities.

The issue CVE-2016-2107 states that:
A MITM attacker can use a padding oracle attack to decrypt traffic when the connection uses an AES CBC cipher and the server support AES-NI. This issue was introduced as part of the fix for Lucky 13 padding attack (CVE-2013-0169). The padding check was rewritten to be in constant time by making sure that always the same bytes are read and compared against either the MAC or padding bytes. But it no longer checked that there was enough data to have both the MAC and padding bytes.

A device is vulnerable to CVE-2016-2108 if it:

- Parses and re-encodes, verifies RSA signatures on X.509 certificates with valid certificates from trusted Certification Authorities

A device is vulnerable to CVE-2016-2107 if it:

- Uses AES-CBC cipher and supports AES-NI

Silver Peak Unity Orchestrator/GMS is NOT susceptible to this vulnerability.

Applicability to Silver Peak deployments: Medium

Recommended Action for Silver Peak Customers:

Silver Peak GMS / Unity Orchestrator:
Silver Peak GMS/Unity Orchestrator is not affected by this vulnerability.

Silver Peak VXOA release for NX/VX/VRX/CPX/EdgeConnect appliances:
It is recommended to upgrade Silver peak NX/VX/VRX/CPX/EdgeConnect to the below mentioned releases to mitigate risk against the vulnerabilities. The patches are in line with the recommendations in the CVE-2016-2107 and CVE-2016-2108 advisories.

Resolution:

Silver Peak Issue Id 30874 tracks the vulnerabilities.

The Resolution for this vulnerability will be in each of the below mentioned branches of release:

Silver Peak VXOA release 8.1.0.0 and later

Silver Peak VXOA release 8.0.4.0 and later

Silver Peak VXOA release 7.3.7.0 and later

Silver Peak VXOA release 6.2.17 and later

Details:

The full details of the advisory are located at-
https://www.openssl.org/news/vulnerabilities.html#y2016

Thank you.

Security Incident Response Team

Silver Peak