Silver Peak Security Advisory

Multiple OpenSSL Vulnerabilities, Published by OpenSSL.org on 10-15-2014

CVE-2014-3513, CVE-2014-3567

Summary:

There is a security advisory from OpenSSL.org, dated October 15, 2014, for OpenSSL vulnerabilities.

There are a total of two (2) vulnerabilities in this advisory:

> CVE-2014-3513, "SRTP Memory Leak"
>
> CVE-2014-3567, "Session Ticket Memory Leak"

Silver Peak VXOA products do not use affected versions of OpenSSL. Customers are not required to take any action on their Silver Peak VXOA products for either of these vulnerabilities.

Silver Peak GMS products are not vulnerable to the first vulnerability, CVE-2014-3513, "SRTP Memory Leak". Customers do not need to take any action for this vulnerability.

For CVE-2014-3567, "Session Ticket Memory Leak", Silver Peak will be issuing a patched release of GMS in the near future. Customers are advised to keep their GMS running on their internal network behind a firewall to mitigate any risk.

Details:

There are two (2) advisories posted by OpenSSL, followed up with advisories published by NIST on Oct 18 2014:

The full advisory for CVE-2014-3513 from NIST, located at http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2014-3513, reads as follows:

Memory leak in d1_srtp.c in the DTLS SRTP extension in OpenSSL 1.0.1 before 1.0.1j allows remote attackers to cause a denial of service (memory consumption) via a crafted handshake message.

The advisory on OpenSSL.org reads as follows:

> A flaw in the DTLS SRTP extension parsing code allows an attacker, who sends a carefully crafted handshake message, to cause OpenSSL to fail to free up to 64k of memory causing a memory leak. This could be exploited in a Denial Of Service attack. This issue affects OpenSSL 1.0.1 server implementations for both SSL/TLS and DTLS regardless of whether SRTP is used or configured. Implementations of OpenSSL that have been compiled with OPENSSL_NO_SRTP defined are not affected. (original advisory). Reported by LibreSSL project.
>
> Fixed in OpenSSL 1.0.1j (Affected 1.0.1i, 1.0.1h, 1.0.1g, 1.0.1f, 1.0.1e, 1.0.1d, 1.0.1c, 1.0.1b, 1.0.1a, 1.0.1)

OpenSSL assigns CVE-2014-3513 a severity level of "High".

The full advisory for CVE-2014-3567 from NIST, located at http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2014-3567, reads as follows:

Memory leak in the tls_decrypt_ticket function in t1_lib.c in OpenSSL before 0.9.8zc, 1.0.0 before 1.0.0o, and 1.0.1 before 1.0.1j allows remote attackers to cause a denial of service (memory consumption) via a crafted session ticket that triggers an integrity-check failure.

The advisory on OpenSSL.org reads as follows:

> When an OpenSSL SSL/TLS/DTLS server receives a session ticket the integrity of that ticket is first verified. In the event of a session ticket integrity check failing, OpenSSL will fail to free memory causing a memory leak. By sending a large number of invalid session tickets an attacker could exploit this issue in a Denial Of Service attack. (original advisory).
>
> Fixed in OpenSSL 1.0.1j (Affected 1.0.1i, 1.0.1h, 1.0.1g, 1.0.1f, 1.0.1e, 1.0.1d, 1.0.1c, 1.0.1b, 1.0.1a, 1.0.1)
>
> Fixed in OpenSSL 1.0.0o (Affected 1.0.0n, 1.0.0m, 1.0.0l, 1.0.0k, 1.0.0j, 1.0.0i, 1.0.0g, 1.0.0f, 1.0.0e, 1.0.0d, 1.0.0c, 1.0.0b, 1.0.0a, 1.0.0)
>
> Fixed in OpenSSL 0.9.8zc (Affected 0.9.8zb, 0.9.8za, 0.9.8y, 0.9.8x, 0.9.8w, 0.9.8v, 0.9.8u, 0.9.8t, 0.9.8s, 0.9.8r, 0.9.8q, 0.9.8p, 0.9.8o, 0.9.8n, 0.9.8m, 0.9.8l, 0.9.8k, 0.9.8j, 0.9.8i, 0.9.8h, 0.9.8g)

OpenSSL assigns CVE-2014-3567 a severity level of “Medium”.

Recommended Action for Silver Peak Customers:

Silver Peak products use the following versions of OpenSSL, none of which are affected:

Silver Peak VXOA:	OpenSSL 0.9.8b
Silver Peak GX-V (6.0.2 and later):	OpenSSL 1.0.0e-fips
Silver Peak GX-V (pre-6.0.2):	OpenSSL 1.0.0b-fips
Silver Peak GX-1100s:	OpenSSL 1.0.0b-fips

Silver Peak VXOA products do not use affected versions of OpenSSL. Customers are not required to take any action on their Silver Peak VXOA products for either of these vulnerabilities.

Silver Peak GMS products are not vulnerable to the first vulnerability, CVE-2014-3513, “SRTP Memory Leak”. Customers do not need to take any action for this vulnerability.

For CVE-2014-3567, “Session Ticket Memory Leak”, Silver Peak will be issuing a patched release of GMS in the near future. Customers are advised to keep their GMS running on their internal network behind a firewall to mitigate any risk.