Silver Peak Security Advisory

SSL 3.0 Vulnerability, a.k.a. “Poodle”, Published by NIST on 10-16-2014

CVE-2014-3566, CVE-2014-3568

Summary:

There is a US-CERT/NIST security advisory originally dated October 14, 2014, last revised on October 16, 2014, for an SSL 3.0 vulnerability, also known as “Poodle”.

There are two (2) vulnerabilities in this advisory:

CVE-2014-3566, “openssl: Padding Oracle on Downgraded Legacy Encryption Attack”

CVE-2014-3568, “Build option no-ssl3 is incomplete”

Silver Peak products do use affected versions of OpenSSL. Therefore, Silver Peak will be issuing patched releases in the near future to address both vulnerabilities. Specifically, the patched releases will disable SSL v3.0 to address CVE-2014-3566. Because the patched release will disable SSL v3.0 at the application level, not at library build time, CVE-2014-3568 will be addressed by default in the upcoming patched releases.

In the meantime, Silver Peak TAC strongly recommends disabling SSL v3.0 on any client machines and on browsers that will be used to manage Silver Peak appliances.

Details:

There are two (2) advisories related to the Poodle vulnerability:

The full advisory for CVE-2014-3566 from NIST, located at http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2014-3566, reads as follows:

The SSL protocol 3.0, as used in OpenSSL through 1.0.1i and other products, uses nondeterministic CBC padding, which makes it easier for man-in-the-middle attackers (MITM) to obtain cleartext data via a padding-oracle attack, also known as the "POODLE" issue.

The exploit is published by OpenSSL at: https://www.openssl.org/~bodo/ssl-poodle.pdf

This CVE has been impact rated with CVSS v2 Base Score of 4.3 (MEDIUM)

For details on NIST impact ratings, browse to:

http://nvd.nist.gov/cvss.cfm?vectorinfo&version=2

The full advisory for CVE-2014-3568 from NIST, located at http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2014-3568, reads as follows:

OpenSSL before 0.9.8zc, 1.0.0 before 1.0.0o, and 1.0.1 before 1.0.1j does not properly enforce the no-ssl3 build option, which allows remote attackers to bypass intended access restrictions via an SSL 3.0 handshake, related to s23_clnt.c and s23_srvr.c.

The advisory on OpenSSL.org reads as follows:

> When OpenSSL is configured with "no-ssl3" as a build option, servers could accept and complete a SSL 3.0 handshake, and clients could be configured to send them. (original advisory). Reported by Akamai Technologies.
>
> 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, 0.9.8f, 0.9.8e, 0.9.8d, 0.9.8c, 0.9.8b, 0.9.8a, 0.9.8)

OpenSSL assigns this CVE a severity of “Low”.

Response from OpenSSL.org

> OpenSSL has added support for TLS_FALLBACK_SCSV to allow applications to block the ability for a MITM attacker to force a protocol downgrade. Some client applications (such as browsers) will reconnect using a downgraded protocol to work around interoperability bugs in older servers. This could be exploited by an active man-in-the-middle to downgrade connections to SSL 3.0 even if both sides of the connection support higher protocols. SSL 3.0 contains a number of weaknesses including POODLE (CVE-2014-3566). See also https://tools.ietf.org/html/draft-ietf-tls-downgrade-scsv-00 and https://www.openssl.org/~bodo/ssl-poodle.pdf
>
> 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, 0.9.8f, 0.9.8e, 0.9.8d, 0.9.8c, 0.9.8b, 0.9.8a, 0.9.8)

> Upcoming Silver Peak patched releases will remove SSL v3.0 support via the Apache configuration within Silver Peak products, therefore obviating the need for implementing OpenSSL’s fix in Silver Peak products.

Recommended Action for Silver Peak Customers:

Silver Peak TAC strongly recommends disabling SSL v3.0 on any client machines and on browsers that will be used to manage Silver Peak products.

Silver Peak products use the following versions of OpenSSL:

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

The CVE listed above is directly related to the following vulnerable OpenSSL versions:

* cpe:/a:openssl:openssl:1.0.0i and previous versions

* cpe:/a:openssl:openssl:1.0.0h

* cpe:/a:openssl:openssl:1.0.0g

* cpe:/a:openssl:openssl:1.0.0f

* cpe:/a:openssl:openssl:1.0.0e

* cpe:/a:openssl:openssl:1.0.0d

* cpe:/a:openssl:openssl:1.0.0c

* cpe:/a:openssl:openssl:1.0.0b

* cpe:/a:openssl:openssl:1.0.0a

* cpe:/a:openssl:openssl:1.0.0:beta5

* cpe:/a:openssl:openssl:1.0.0:beta4

* cpe:/a:openssl:openssl:1.0.0:beta3

* cpe:/a:openssl:openssl:1.0.0:beta2

* cpe:/a:openssl:openssl:1.0.0:beta1

* cpe:/a:openssl:openssl:1.0.0