Silver Peak Security Advisory

Logjam Vulnerability, Published by NIST on 05/20/2015

CVE-2015-4000

Summary:

US-CERT/NIST advisory for CVE-2015-4000 is dated 05/20/2015. The advisory is about the possibility of a cipher downgrade attack for TLS 1.2 and earlier versions, using the man-in-the-middle technique.

The TLS protocol 1.2 and earlier, when a DHE_EXPORT cipher suite is enabled on a server but not on a client, does not properly convey a DHE_EXPORT choice, which allows man-in-the-middle attackers to conduct cipher-downgrade attacks by rewriting a ClientHello with DHE replaced by DHE_EXPORT and then rewriting a ServerHello with DHE_EXPORT replaced by DHE, also known as the "Logjam" issue.

Silver Peak products use the following versions of OpenSSL:

Silver Peak VXOA: OpenSSL 0.9.8b

Silver Peak VXOA appliances are susceptible to this vulnerability, and the patch for resolving this is detailed under the heading, Resolution.

Details:

CVE provides information on the advisory and is located at:
https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2015-4000

The full advisory is located at https://weakdh.org/ and reads as follows:

Diffie-Hellman key exchange is a popular cryptographic algorithm that allows Internet protocols to agree on a shared key and negotiate a secure connection. It is fundamental to many protocols including HTTPS, SSH, IPsec, SMTPS, and protocols that rely on TLS.

We have uncovered several weaknesses in how Diffie-Hellman key exchange has been deployed:

1. **Logjam attack against the TLS protocol.** The Logjam attack allows a man-in-the-middle attacker to downgrade vulnerable TLS connections to 512-bit export-grade cryptography. This allows the attacker to read and modify any data passed over the connection. The attack is reminiscent of the FREAK attack, but is due to a flaw in the TLS protocol rather than an implementation vulnerability, and attacks a Diffie-Hellman key exchange rather than an RSA key exchange. The attack affects any server that supports DHE_EXPORTciphers, and affects all modern web browsers. 8.4% of the Top 1 Million domains were initially vulnerable.

2. **Threats from state-level adversaries.** Millions of HTTPS, SSH, and VPN servers all use the same prime numbers for Diffie-Hellman key exchange. Practitioners believed this was safe as long as new key exchange messages were generated for every connection. However, the first step in the number field sieve—the most efficient algorithm for breaking a Diffie-Hellman connection—is dependent only on this prime. After this first step, an attacker can quickly break individual connections.

   We carried out this computation against the most common 512-bit prime used for TLS and demonstrate that the Logjam attack can be used to downgrade connections to 80% of TLS servers supporting DHE_EXPORT. We further estimate that an academic team can break a 768-bit prime and that a nation-state can break a 1024-bit prime. Breaking the single, most common 1024-bit prime used by web servers would allow passive eavesdropping on connections to 18% of the Top 1 Million HTTPS domains. A second prime would allow passive decryption of connections to 66% of VPN servers and 26% of SSH servers. A close reading of published NSA leaks shows that the agency's attacks on VPNs are consistent with having achieved such a break.

Full Technical Paper

Imperfect Forward Secrecy: How Diffie-Hellman Fails in Practice

Link to the paper: https://weakdh.org/imperfect-forward-secrecy-ccs15.pdf

NIST has added the vulnerability summary for this CVE to their National Cyber Awareness System database:

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-4000

Recommended Action for Silver Peak Customers:

Silver Peak VXOA appliances:
Silver Peak VXOA appliances are affected by this vulnerability. To mitigate risk, Silver Peak recommends upgrading VXOA appliances to the releases listed in RESOLUTION. The patch is in line with the recommendation in the CVE-2015-4000 advisory.

Resolution:

Silver Peak Issue Id 26920 tracks this vulnerability.

The resolution for this vulnerability is in each of the following release branches:

- **VXOA 6.2.12.0 and later releases**
- **VXOA 7.2.1.0 and later releases**
- **VXOA 7.3.0.0 and later releases**