Silver Peak Security Advisory

Drown attack vulnerability

CVE-2016-0800, published by NIST on 03/01/2016

Summary:

US-CERT/NIST advisory for CVE-2016-0800 is dated 03/01/2016. The advisory concerns the SSLv2 protocol, as used in OpenSSL before 1.0.1s and 1.0.2 before 1.0.2g and other products These versions require a server to send a ServerVerify message before establishing that a client possesses certain plaintext RSA data, which makes it easier for remote attackers to decrypt TLS ciphertext data by leveraging a Bleichenbacher RSA padding oracle, aka a "DROWN" attack.

A server is vulnerable to DROWN if:

- It allows SSLv2 connections.
  or:
- Its private key is used on any other server that allows SSLv2 connections, even for another protocol.

Silver Peak VXOA does not support SSLv2
Silver Peak Orchestrator (GMS) supports SSLv2

Silver Peak Orchestrator (GMS) is vulnerable to this vulnerability.

Silver Peak VXOA appliances are not susceptible to this vulnerability.

The patch to resolve the vulnerability is detailed under 'Resolution' heading below.

Details:

CVE provides information on the advisory and is located at: https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-0800

The full advisory located at https://drownattack.com/ reads as follows:

DROWN is a serious vulnerability that affects HTTPS and other services that rely on SSL and TLS, some of the essential cryptographic protocols for Internet security. These protocols allow everyone on the Internet to browse the web, use email, shop online, and send instant messages without third-parties being able to read the communication.

DROWN allows attackers to break the encryption and read or steal sensitive communications, including passwords, credit card numbers, trade secrets, or financial data. Our measurements indicate 33% of all HTTPS servers are vulnerable to the attack.

What can the attackers gain?

Any communication between users and the server. This typically includes, but is not limited to, usernames and passwords, credit card numbers, emails, instant messages, and sensitive documents. Under some common scenarios, an attacker can also impersonate a secure website and intercept or change the content the user sees.

Who is vulnerable?

Websites, mail servers, and other TLS-dependent services are at risk for the DROWN attack, and many popular sites are affected. We used Internet-wide scanning to measure how many sites are vulnerable:

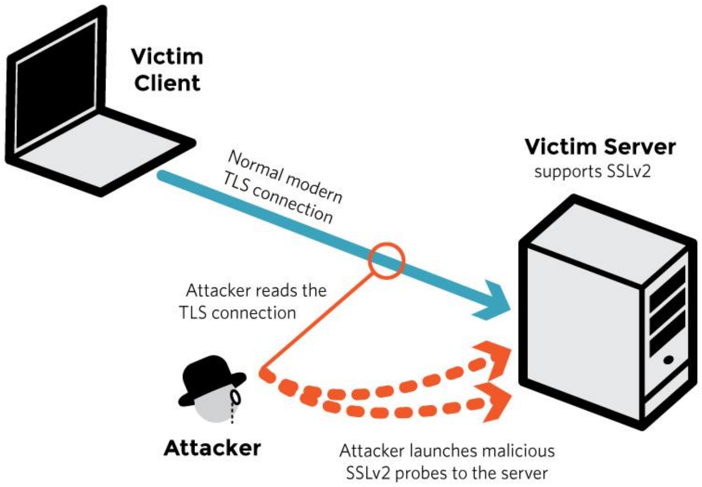
Vulnerable at Disclosure (March 1)	
HTTPS — Top one million domains	25%
HTTPS — All browser-trusted sites	22%
HTTPS — All sites	33%

Operators of vulnerable servers need to take action. There is nothing practical that browsers or end-users can do on their own to protect against this attack.

Is my site vulnerable?

Modern servers and clients use the TLS encryption protocol. However, due to misconfigurations, many servers also still support SSLv2, a 1990s-era predecessor to TLS. This support did not matter in practice, since no up-to-date clients actually use SSLv2. Therefore, even though SSLv2 is known to be badly insecure, until now, merely supporting SSLv2 was not considered a security problem, because clients never used it.

DROWN shows that merely supporting SSLv2 is a threat to modern servers and clients. It allows an attacker to decrypt modern TLS connections between up-to-date clients and servers by sending probes to a server that supports SSLv2 and uses the same private key.


Victim Client
Normal modern TLS connection
Victim Server
supports SSLv2
Attacker reads the TLS connection
Attacker
Attacker launches malicious SSLv2 probes to the server

A server is vulnerable to DROWN if:

- It allows SSLv2 connections. This is surprisingly common, due to misconfiguration and inappropriate default settings. Our measurements show that 17% of HTTPS servers still allow SSLv2 connections.
  or:

- Its private key is used on any other server that allows SSLv2 connections, even for another protocol. Many companies reuse the same certificate and key on their web and email servers, for instance. In this case, if the email server supports SSLv2 and the web server does not, an attacker can take advantage of the email server to break TLS connections to the web server. When taking key reuse into account, an additional 16% of HTTPS servers are vulnerable, putting 33% of HTTPS servers at risk.

How do I protect my server?
To protect against DROWN, server operators need to ensure that their private keys are not used anywhere with server software that allows SSLv2 connections. This includes web servers, SMTP servers, IMAP and POP servers, and any other software that supports SSL/TLS. You can use the form above to check whether your server appears to be exposed to the attack.
Disabling SSLv2 can be complicated and depends on the specific server software. We provide instructions here for several common products:
OpenSSL: OpenSSL is a cryptographic library used in many server products. For users of OpenSSL, the easiest and recommended solution is to upgrade to a recent OpenSSL version. OpenSSL 1.0.2 users should upgrade to 1.0.2g. OpenSSL 1.0.1 users should upgrade to 1.0.1s. Users of older OpenSSL versions should upgrade to either one of these versions. More details can be found in this OpenSSL blog post.
(Updated March 13th, 16:00 UTC) Microsoft IIS (Windows Server): Support for SSLv2 on the server side is enabled by default only on the OS versions that correspond to IIS 7.0 and IIS 7.5, namely Windows Vista, Windows Server 2008, Windows 7 and Windows Server 2008R2. This

support can be disabled in the appropriate SSLv2 subkey for 'Server', as outlined in KB245030. Even if users have not taken the steps to disable SSLv2, the export-grade and 56-bit ciphers that make DROWN feasible are not supported by default.
Network Security Services (NSS): NSS is a common cryptographic library built into many server products. NSS versions 3.13 (released back in 2012) and above should have SSLv2 disabled by default. (A small number of users may have enabled SSLv2 manually and will need to take steps to disable it.) Users of older versions should upgrade to a more recent version. We still recommend checking whether your private key is exposed elsewhere, using the form above.
Other affected software and operating systems:
Instructions and information for: Apache, Postfix, Nginx, Debian, Red Hat
Browsers and other clients: There is nothing practical that web browsers or other client software can do to prevent DROWN. Only server operators are able to take action to protect against the attack.

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

https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2016-0800

Recommended Action for Silver Peak Customers:

Silver Peak GMS (Orchestrator) product:
Silver Peak GMS (Orchestrator) is affected by this vulnerability. It is recommended to upgrade GMS to below mentioned releases to mitigate risk against the vulnerability. The patch is in line with the recommendation in the CVE-2016-0800 advisory.

Silver Peak VXOA appliances:
Silver Peak VXOA appliances are not affected by this vulnerability.

Resolution:

Silver Peak Issue Id 29789 tracks this vulnerability.

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

Orchestrator release 7.3.7 and later

Orchestrator (GMS) release 8.0.1 and later

Orchestrator (GMS) release 8.1.0 and later