CERT-MU Security Alert

CERT-MU

THE DROWN ATTACK - MILLIONS OF OPENSSL SECURED WEBSITES AT RISK

Original Issue Date: 02nd March, 2016

Severity Rating: High

Description:

Security researchers have uncovered an attack dubbed as **"DROWN"** that can compromise encrypted network traffic in a matter of hours. Drown (**D**ecrypting **R**SA with **O**bsolete and **W**eakened E**N**cryption) attack successfully decrypts TLS (transport layer security) sessions by exploiting a vulnerability in the older SSL v2 protocol that exposes private RSA keys.

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.

Impact of the attack

The attack can allow remote attackers to get hold of any communication between users and the servers, including usernames, passwords, credit card details, instant messages and other sensitive documents. Additionally, an attacker can also impersonate a secure website, intercept or change the content the user sees

Vulnerable websites

Websites, mail servers, and other TLS-dependent services are at risk for the DROWN attack, and many popular sites are affected.

How a website is vulnerable to DROWN?

A server is vulnerable to DROWN if:

1. It allows SSLv2 connections - due to misconfiguration and inappropriate default settings.

   OR

2. 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.

Testing the DROWN Attack

Users can find if their website is vulnerable to this critical security hole using the DROWN attack test site: https://test.drownattack.com/

Workarounds

OpenSSL has issued a patch to fix the vulnerability and has disabled the SSLv2 protocol by default, as well as removing SSLv2 EXPORT ciphers. It is strongly advised not to use SSLv2.

- OpenSSL 1.0.2 users should upgrade to 1.0.2g.
- OpenSSL 1.0.1 users should upgrade to 1.0.1s.

More detail about the patch is available on:

https://www.openssl.org/news/secadv/20160301.txt

Recommendations

To protect against the DROWN attack, 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.

The following instructions are provided for the following 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 on: OpenSSL blog post

Microsoft IIS (Windows Server): IIS versions 7.0 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.)

It is recommended to check whether your private key is exposed elsewhere, using the form above. IIS versions below 7.0 are no longer supported by Microsoft and should be upgraded to supported versions.

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.

Please note that the members who do not want to receive the security alert, they can unsubscribe from CERT-MU mailing list by sending an e-mail to the following address: unsubscribe@cert.ncb.mu

For more information please contact CERT-MU team on:

Hotline No: (+230) 800 2378
Fax No: (+230) 208 0119
Gen. Info. : contact@cert.ncb.mu
Incident: incident@cert.ncb.mu
Website: http://cert-mu.org.mu