National Cyber Security Centre
Ministry of Security and Justice

Disable SSL 2.0 and upgrade OpenSSL

Attacker can use DROWN attack methods to break TLS security

Factsheet FS-2016-03 | version 1.0 | 3 maart 2016

On 1 March, a group of researchers presented the DROWN attack methods for TLS. An attacker uses DROWN to abuse servers that still support SSL 2.0. Servers that run a vulnerable version of OpenSSL can be abused in the same way, regardless of whether they support SSL 2.0. An attacker who is able to intercept network traffic that is secured with TLS, may attempt to decrypt this traffic using the vulnerable server. This allows him to inspect the traffic.

The NCSC advises to always configure TLS on the basis of the IT security guidelines for Transport Layer Security. Therefore, disable SSL 2.0, install the most recent updates of OpenSSL and prefer cipher suites that provide forward secrecy on all servers.

Target audience

IT administrators, information security professionals, IT managers

This factsheet was written in collaboration with:

National Communications Security Agency

Background

Transport Layer Security is the most frequently used protocol for securing internet connections. Using TLS, a client and server can set up a cryptographically secured tunnel. After setting up the tunnel, client and server can communicate securely with each other.

SSL 2.0 is a very old version of TLS. It has been known for a long time that SSL 2.0 contains vulnerabilities. However, some people assumed that offering SSL 2.0 did not pose an additional risk. As a consequence, many servers still support SSL 2.0, in addition to new more secure options.

OpenSSL is a popular programming library for implementing the functionality of TLS. TLS is a complex protocol. Most applications therefore use a programming library to implement the protocol. Especially server software often employs OpenSSL for this purpose.

What is the matter?

On 1 March 2016, a group of researchers presented a number of new attack methods for TLS.[1] They have named these techniques DROWN. DROWN stands for 'Decrypting RSA with Obsolete and Weakened eNcryption'.

An attacker uses DROWN to abuse servers that still support SSL 2.0. This still happens relatively often, for example on mail servers. It does not matter in this case which programming library the server employs.

Servers that run a vulnerable version of OpenSSL can be abused in the same way. There, it does not matter if the administrator has disabled SSL 2.0 in the configuration of OpenSSL. This vulnerability in OpenSSL has been resolved on 28 January 2016.[2] These versions are no longer vulnerable, if SSL 2.0 is disabled in the configuration.

An attacker who is able to intercept network traffic that is secured with TLS, may attempt to decrypt this traffic using the vulnerable server. This allows him to inspect the traffic. This requires that the vulnerable server and the server that exchanges TLS traffic have the same private key for their TLS certificate. In particular, these can be both the same server. It does not matter which version of TLS was used to secure the intercepted TLS traffic.

The researchers have not yet published their source code for executing DROWN. This makes it considerably harder to execute the attack. Only a expert attacker will be able to execute the attack based on just the research report. The researchers have indicated that they will not release their source code for now.

What could happen?

To perform a DROWN attack, an attacker will intercept about one thousand TLS sessions. These sessions should all be to servers that use the same private key as the vulnerable server. Also, none of these sessions should use forward secrecy. Then, he uses the information from the intercepted sessions to establish a few tens of thousands connections to the vulnerable server. By cleverly manipulating the vulnerable server, the attacker is able to recover the session key of on average one of the TLS sessions.[3]

Using the recovered session key, the attacker can decrypt one of the thousand intercepted TLS sessions. He then possesses the entire contents of this session. Sensitive data that should have been secured using TLS are then visible to the attacker. The attacker cannot decide beforehand which of the thousand sessions he will decrypt. He also cannot break more of the sessions by further efforts.

The researchers state that executing the attack costs around € 400 and eight hours of calculations. This is the cost of breaking on average one of the thousand TLS sessions.

Special DROWN

A special variant of the attack, 'special DROWN', is much easier and cheaper to execute. The attacker can then also break connections with forward secrecy and impersonate the vulnerable server. This variant requires that the vulnerable server uses an outdated version of OpenSSL. Versions from 1.0.2a, 1.0.1m, 1.0.0r and 0.9.8zf are not vulnerable. Updates to these versions have been published on 19 March 2015.[4]

Breaking one in a thousand sessions does not sound very shocking, but enough scenarios exist in which every session is sensitive. For example, when login credentials are exchanged, it does not matter to the attacker which of the user's sessions he is able to break. After all, each session contains the same login credentials.

What does the NCSC recommend?

The NCSC advises to always configure TLS following the IT security guidelines for Transport Layer Security.[5] Therefore, disable SSL 2.0, install the most recent updates of OpenSSL[6] and prefer cipher suites that provide forward secrecy on all servers.

Disabling SSL 2.0 on servers should not have a negative impact on the functioning of IT systems. SSL 2.0 has been obsolete for so long that hardly any systems exist that require it. However, it may be the case that the option to disable SSL 2.0 is lacking. For alternative measures, see the frame 'Secure through network detection and firewalling'.

Updating OpenSSL to the most recent version is possible for all servers that run an operating system that is still supported. Versions from 1.0.2f and 1.0.1r are no longer vulnerable. Some operating system vendors offer an old version, but 'backport' the security updates to this version. On some devices it is not possible to install the security updates. See the frame 'Secure through network detection and firewalling' for alternative measures.

[1] https://drownattack.com
[2] CVE-2015-3197, http://openssl.org/news/secadv/20160128.txt
[3] The number of session keys that the attacker recovers depends on the number of intercepted sessions. With one thousand sessions, the expected number of recovered session keys is one.
[4] CVE-2015-0703, http://openssl.org/news/secadv/20160301.txt
[5] See https://www.ncsc.nl/actueel/whitepapers/ict-beveiligingsrichtlijnen-voor-transport-layer-security-tls.html.
[6] Strictly speaking, the vulnerabilities mentioned here have been resolved in the second to latest version of OpenSSL (released on 28 January 2016). It is nonetheless always a good idea to upgrade to the most recent version.

Secure through network detection and firewalling

Using network detection, the DROWN attack method can be detected. The fact is, the method requires a few tens of thousands connections based on SSL 2.0 to the vulnerable server. Should you detect many connections based on SSL 2.0 in your network traffic, this could indicate a DROWN attack is under way.

DROWN attacks can be prevented by blocking all network traffic based on SSL 2.0 to possibly vulnerable servers. After all, legitimate SSL 2.0 traffic is exceedingly scarce. This measure may however be quite high-maintenance. Therefore, only use it as an alternative to regular measures (disabling SSL 2.0 and updating OpenSSL).

Prevent broad reuse of private keys between servers. Is a server vulnerable to the DROWN attack method, then all servers that use the same private key are vulnerable as well. Particularly, take care to prevent third parties who possess private keys to your certificates from using the same private keys as you use on your systems. After all, you have only limited control over the configuration of servers of these third parties. Examples of such parties are vendors of anti-DDoS services or content delivery networks (CDNs) for websites.

It is not necessary to replace TLS certificates as a consequence of the DROWN attack method. After all, the attacker does not gain access to the private key of the certificate.

It is not possible to apply mitigating measures on the client side of a TLS connection. The vulnerabilities only apply to the server side.

Perspective for action

- Make an inventory of all servers in your organisation that offer TLS. Group these servers based on their reuse of private keys. If server A and server B share a private key, then server A and B are in the same group. Include servers of third parties in this inventory if they share private keys with systems that you maintain.
- Apply the main advice to each group of servers: disable SSL 2.0 on all servers and upgrade OpenSSL to a version published after 28 January 2016.[7]
- Is it impossible to apply the main advice to the group of servers, then configure your firewall to block SSL 2.0 traffic to all servers in the group for which you do not apply the main advice.

[7] See also https://www.ncsc.nl/dienstverlening/response-op-dreigingen-en-incidenten/beveiligingsadviezen/NCSC-2016-0196+1.01+Kwetsbaarheid+ontdekt+in+SSL+2.0.html.

Publication
National Cyber Security Centre (NCSC)
P.O. Box 117, 2501 CC The Hague
Turfmarkt 147, 2511 DP The Hague
+31 (70) 751 5555

More information
www.ncsc.nl
info@ncsc.nl
@ncsc_nl

FS-2016-03 | version 1.0 | 3 March 2016