Security Advisory Report - OBSO-1603-02

DROWN: Breaking TLS using SSLv2 (CVE-2016-0800)

Creation Date: 2016-03-02
Last Update: 2016-10-21

Summary

On March 1st, 2016 new attack methods were disclosed that affect a significant amount of SSL/TLS based services, called "DROWN" (**D**ecrypting **R**SA using **O**bsolete and **W**eakened e**N**cryption). Mitre has assigned CVE-2016-0800 to this issue.

This advisory summarizes the impact of CVE-2016-0800 for customers using products of Unify.
Risk for Unify products: none to low
No products of Unify in current/actively sustained versions are considered vulnerable, **except (with low risk): OpenScape 4000 Assistant V7 R2**

Vulnerability Details

The "DROWN" (short for Decrypting RSA using Obsolete and Weakened eNcryption) attack (CVE-2016-0800) applies the Bleichenbacher RSA padding oracle to an SSLv2 enabled TLS server. This may allow the attacker to decrypt data from other TLS sessions (even if those sessions have been negotiated using up-to-date TLS protocol versions and cipher suites).

Any TLS server may be vulnerable to "DROWN" if it allows SSLv2 connections, or if its private key is co-used on any other server that allows SSLv2 connections.
For more information refer to the original publication at https://drownattack.com/.
Direct link to the research paper: https://drownattack.com/drown-attack-paper.pdf.

While "DROWN" describes a weakness that is inherently associated with the SSLv2 **protocol**, OpenSSL has disclosed further details, that refer to **implementation**-specific vulnerabilities in the OpenSSL code. These vulnerabilities leverage the impact of DROWN on TLS servers that are based on OpenSSL by making potential attacks easier to succeed.
Specifically, the following issues apply to different versions of OpenSSL:

- SSLv2 doesn't block disabled ciphers (CVE-2015-3197)
- Divide-and-conquer session key recovery in SSLv2 (CVE-2016-0703)
- Bleichenbacher oracle in SSLv2 (CVE-2016-0704)

Affected Products

Most Unify products are not affected by CVE-2016-0800, CVE-2015-3197, CVE-2016-0703, or CVE-2016-0704.
Unify products do not support the SSLv2 protocol in all versions that are currently actively sustained, except:

1. OpenScape 4000 Assistant V7 R2 (risk = low)
A bug in the TLS configuration for OpenScape 4000 Assistant re-enabled the SSLv2 and SSLv3 protocols on port tcp/9980 (TSKA, TSDM services), starting with V7 R2.0.0. OpenScape 4000 Assistant V7 R1 or earlier were not affected.
The risk is considered as low. Note that the TLS certificate on the Assistant server is used for both the TSKA, TSDM services (port tcp/9980) and the Webbased-Management (WBM, port tcp/443). Therefore, a potential attacker may be able to decrypt the session between a legitimate administrator's browser and the WBM. This however requires the attacker to intercept hundreds of individual WBM sessions, and to send many data probes against the vulnerable port tcp/9980.
In reasonably protected network environments, where only a limited set of administrators have access to the OpenScape Assistant's interfaces and where administrative sessions occur only occasionally, a successful exploit is considered very unlikely.
Malicious attempts to exploit CVE-2016-0800 may be detected by examining unusual high TCP/TLS traffic (at unusual times) to port tcp/9980.

2. OpenScape Business and OpenScape Office (risk = none)
OpenScape Business and OpenScape Office support an integrated DLS service (called "DLI") that provides a TLS interface on port tcp/18443 for initial deployment of phone software to attached OpenStage or OpenScape Desk Phone HFA devices (the DLS-WPI "Default Mode" interface). The "Default Mode" does not provide any server authentication by design. Therefore, although the DLI still offers SSLv2/SSLv3 at this interface, this configuration does not add any additional attack vector or additional risk to customer installations.
For secure management of attached HFA devices it is recommended to operated a separate DLS service (OpenScape Deployment Service) configured in "Secure Mode".
For more information see the Security Checklist of OpenStage / OpenScape Desk Phone IP HFA V3, chapter 4.2.3 (Hardening of DLS Interface).

Recommended Actions

OpenScape 4000 Assistant V7 R2:
Update to OpenScape 4000 Assistant V7 R2.20.5 (HF004537, GA release date: 2016-10-21) which removes the SSLv2/SSLv3 support on port tcp/9980, or to any later version.

In general, review the list of TLS servers in your environment and remove support of SSLv2 protocol wherever it is still enabled today. Avoid the concurrent use of the same private keys/TLS server certificates on different protocols or servers.

References

- Research paper: DROWN: Breaking TLS using SSLv2
- DROWN "landing page": https://drownattack.com/
- OpenSSL Software Foundation:
  - OpenSSL Security Advisory [1st March 2016]
  - OpenSSL Security Advisory [28th Jan 2016]

Revision History

2016-03-02: Initial release

2016-10-21: Update 01:

- Added information about affected OpenScape 4000 Assistant V7 R2
- Added note for OpenScape Business and OpenScape Office

Advisory ID: OBSO-1603-02 (a=140), status: update release
Security Advisories are released as part of Unify's Vulnerability Intelligence Process. For more information see https://www.unify.com/security/advisories.

Contact and Disclaimer
OpenScape Baseline Security Office
obso@unify.com

Mies-van-der-Rohe Str. 6, D-80807 München
www.unify.com