Security Advisory Report - OBSO-1410-02

SSL 3.0 "POODLE" vulnerability (CVE-2014-3566)

Creation Date: 2014-10-17
Last Update: 2014-10-17

Summary

On Oct. 14, 2014 a new method to exploit a vulnerability in the SSL (Secure Socket Layer) version 3.0 was published. A man-in-the-middle attacker may be able to decrypt portions of the data that is exchanged between the client and the server. The attack is known as "POODLE" (Padding Oracle On Downgraded Legacy Encryption).

Most Unify products are not affected as they are not using SSL 3.0. The risk for some Unify products is rated low.
The advisory will be updated as soon as new information is available.

Vulnerability Details

SSL 3.0 is an industry-wide legacy standard for encrypted communication that has been superseded by TLS (Transport Layer Security) since the definition of TLS 1.0 in 1999. For backward compatibility reasons, SSL 3.0 is still offered as a fallback option in many implementations of the TLS protocol.
In cases where both the TLS client and the TLS server support fallback to SSL 3.0, an attacker may enforce this downgrade to SSL 3.0. In the following encrypted communication, a padding oracle attack can result in a bytewise decryption of a chosen part in the ciphertext (with a success rate of average 256 attempts per byte).

For a successful exploitation, the attacker must

- be able to intercept and modify the network traffic between the client and the server (aka "man-in-the-middle")
- force a downgrade to establish the client-server connection with SSL 3.0 (by simulating network glitches during the TLS handshake) and to use a block cipher in CBC mode (such as 3DES_EDE_CBC)
- force the client to repeatedly send a data package that contains a secret (such as the client's current session cookie) - for example by injecting malicious javascript code into the client's browser session
- after successful decryption of one byte of the secret: force the client to vary the position of the secrect within the data package (to continue with repeated decryption attempts against the next byte of the secret, until the whole secret becomes known to the attacker)

CVSS Scores:

- Base Score: 2.6, Temporal Score: 2.3
- CVSS v2 Vector (AV:N/AC:H/Au:N/C:P/I:N/A:N/E:F/RL:W/RC:C)

Mitre (cve.mitre.org) has assigned the id CVE-2014-3566 to this issue.

Affected Products

The SSL 3.0 protocol was considered as deprecated already earlier and before the "POODLE" attack became known. Therefore, most Unify products have removed their support for SSL 3.0 as part of ongoing security improvements required by Unify's Baseline Security Policy.

Unify is currently investigating the remaining exceptions. The advisory will be updated as soon as new information is available.

The following products offer SSL 3.0 during TLS connection setup; associated connections may be vulnerable to the "POODLE" attack:

1. OpenScape Branch and OpenScape SBC (all versions):
In **SIP-TLS connections**, the fallback from TLS to SSL is offered as options ("SSLv23" and "SSLv3") in the configuration of Certificate Profiles for TLS. We recommend to check your current systems settings and configure the option "TLSv1" instead. For details refer to the section "How to Create, Edit and Delete Certificate Profiles" in the administrator manual of OpenScape Branch and OpenScape SBC.
This recommendation will also be included in an update of the corresponding Security Checklists.
The deprecated options will be removed in later releases of the products.
The **Webbased Management Interfaces (https)** of OpenScape Branch and OpenScape SBC have removed SSL 3.0 by default in all versions and are therefore not vulnerable (mode: "Secure web management").
Note that the deactivation of the mode "Secure web management" would enable the support of SSL 3.0 and is therefore not recommended.

2. RG 8700 Gateway:
In **SIP-TLS connections** the gateway offers TLS by default, but also SSL as fallback protocol.
An exploit is not possible, provided that the systems or devices that connect with RG 8700 via SIP-TLS have removed their SSL 3.0 support.

3. OpenScape Contact Center Call Director SIP Service (CDSS):
The webbased management interface of CDSS offers SSL 3.0 as fallback protocol.
An exploit is not possible, provided that administrators accessing the CDSS web interface have removed the SSL 3.0 support in their browsers. Refer to the individual browser vendor's recommendations - a collection of links is provided in the "References" section below.
The support of SSL 3.0 will be removed as part of the next fix release for CDSS (V8 R2.10).

Products confirmed as not vulnerable, as they only support TLS, but no version of the SSL protocol:

- OpenScape Voice V6, V7, V8
- HiPath/OpenScape 4000 V6, V7 - Minimum required versions are:
  - V6 R2: V6 R2.16.0 - refer to Security Advisory OBSO-1407-02 for more information
  - V7 R1: all versions - SSL support was removed in V7 R0.12.4
- OpenStage and OpenScape Desk Phone IP
  (Note: older VoIP phones "optiPoint" and "OpenStage 5" which are beyond End of SW support do not support SSL 3.0 as well in their latest versions)
- OpenScape UC Applications

Microsoft Windows-based application server products and end-user applications:
Products such as OpenScape Xpressions, OpenScape Web Collaboration OpenScape Deployment Service have removed SSL support as well and are therefore not affected.
In certain parts (for example the web interface of OpenScape WebCollaboration), the products rely on the native Windows implementation and configuration of the TLS protocol, where SSL 3.0 is currently enabled by default.
We recommend to follow the advise from Microsoft and disable the support of SSL 3.0 on all Windows servers and clients as described in the Microsoft Security Advisory 3009008
There are no known impacts to Unify products running on Windows.

Recommended Actions

Unify's OpenScape Baseline Security Office agrees with the common public opinion and recommends all customers to remove the support of the SSL protocol on all systems, wherever possible and feasible.

In the context of Unify products, please see the individual hints in the section "Affected Products" above.

References

Initial publication as disclosed on 2014-10-14:

- https://www.openssl.org/~bodo/ssl-poodle.pdf

Selection of related vendor advisories:

- Microsoft Windows Server and Clients, and Internet Explorer browser: Microsoft Security Advisory 3009008
- Mozilla Firefox browser: Mozilla Security Blog
- Google Chrome browser: Online Security Blog

Mitre:

- http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-3566

NVD:

- http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2014-3566

Internet Engineering Task Force (IETF):

- RFC 6101 (SSL 3.0)
- RFC 2246 (TLS 1.0)

Revision History

2014-10-17: Initial release

Advisory ID: OBSO-1410-02 (a=94), status: general 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

The information provided in this document contains merely general descriptions or characteristics of performance which in case of actual use do not always apply as described or which may change as a result of further development of the products. An obligation to provide the respective characteristics shall only exist if expressly agreed in the terms of contract. Availability and technical specifications are subject to change without notice.
Unify, OpenScape, OpenStage and HiPath are registered trademarks of Unify Software and Solutions GmbH & Co. KG.

All other company, brand, product and service names are trademarks or registered trademarks of their respective holders.