Security Advisory Report - OBSO-1408-01

openSSL TLS Client Denial of Service vulnerability (CVE-2014-3509)

Creation Date: 2014-08-12
Last Update: 2014-09-26

Summary

On August 6th, 2014, the OpenSSL team published a security advisory that addresses nine vulnerabilities. Among these vulnerabilities, only **CVE-2014-3509** is relevant for the Unify product portfolio.
The risk is rated as low. The updates for affected Unify products will be provided as part of the regular release cycle.

Unify products are not affected by all other reported vulnerabilities (CVE-2014-3505, CVE-2014-3506, CVE-2014-3507, CVE-2014-3508, CVE-2014-3510, CVE-2014-3511, CVE-2014-3512, CVE-2014-5139).

This advisory is therefore released mainly for information purposes.

Vulnerability Details

CVE-2014-3509:
A race condition exists in OpenSSL that affects multithreaded TLS client applications when processing serverhello messages. An attacker could use this vulnerability to cause the TLS client to crash, resulting in a denial of service.
This potentially affects the administration tool HiPath/OpenScape 4000 Expert Access ("ComWin") or any 3rd party software that uses the SecM.dll or the Mpci.lib to access a HiPath/OpenScape 4000 Assistant.
For a successful attack the attacker's system must pretend to be a legitimate HiPath/OpenScape 4000 Assistant server.

Risk level: low
CVSS v2 Base Score: 2.1 (AV:N/AC:H/Au:S/C:N/I:N/A:P)

Affected Products

The following Unify products are affected with low risk:

- Libraries as delivered with Hipath/OpenScape 4000 Assistant for use in 3rd party administration tools and applications:
  - SecM.dll - Solution available: update to version 7.1.0.0 (release date 2014-08-13) or higher
  - Mpci.lib - Solution available: update to version 1.7 (release date 2014-08-15) or higher
- HiPath 4000 Expert Access - **Solution available: update to version V5 R0.121.0 (release date 2014-09-25)** or higher

Recommended Actions

Users of Hipath 4000 Expert Access or similar administration tools should verify that they connect to legitimate HiPath/OpenScape 4000 Assistant servers only.
An unexpected crash of these applications while the tool is being connected with a HiPath/OpenScape 4000 Assistant may be an indicator of a successful attack using CVE-2014-3509. Customers that are affected by this issue should

- update the tool to the latest released version (as listed above) and/or
- report the problem to Unify using the normal product support process.

References

External links:

- openSSL: https://www.openssl.org/news/secadv_20140806.txt
- Mitre: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-3509

Revision History

2014-08-12: Initial release
2014-08-26: Update 01: Fix releases available for SecM.dll, Mpci.lib
2014-09-26: Update 02: Fix release available for HiPath 4000 Expert Access

---

Advisory ID: OBSO-1408-01 (a=88), 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