# Security Advisory Report - OBSO-1404-02

## openSSL "Heartbleed" vulnerability (CVE-2014-0160)

Creation Date: 2014-04-11
Last Update: 2014-05-02

## Summary

On April 7, 2014, a vulnerability in the openSSL implementation of the SSL/TLS protocol was disclosed that affects many products and online services in the Internet. openSSL is a widely-used open source cryptographic software library, also included in various products of Unify. This advisory summarizes the impact of this vulnerability for customers using products of Unify.

Unless specified otherwise, the risk for a specific vulnerable product of Unify is rated as **medium**.
**Important Update, 2014-05-02**: Corrections are now available for all Unify products that are known to be affected.

## Vulnerability Details

A missing bounds check in the handling of the TLS heartbeat extension in openSSL versions 1.0.1 to 1.0.1f could allow an unauthenticated, remote attacker to retrieve memory in chunks of 64 kilobytes from a connected client or server. Thereby, sensitive information could potentially be disclosed, such as the private key of the system's TLS server certificate, or usernames/passwords that were used during logon in a TLS session.

Mitre (cve.mitre.org) has assigned the id CVE-2014-0160 to this issue.
CVSS v2 Scores:

- Base Score 5.0, Temporal Score 5.0
  (AV:N/AC:L/Au:N/C:P/I:N/A:N/E:H/RL:U/RC:C)

The risk depends on the sensitivity of the data that may be disclosed by exploiting the Heartbleed vulnerability on a certain system, and what further attacks can be enabled based on the stolen information.
The product-specific details are therefore listed in the section "Affected Products" below.

***Note:***
*Solutions from Unify may use or be based on various products from other vendors ("third-party products") that are not included in the core Unify product portfolio, such as network components, operating systems, video systems or security applications. These products are not monitored as part of Unify's Vulnerability Intelligence Process and are therefore not covered by this Advisory.*
*However, for your additional support we have collected important information about the impact of CVE-2014-0160 for some of these systems in an appendix to this advisory (OBSO-1404-02-A). We recommend that you check the third-party advisories for potential updates regularly, and wherever possible subscribe to the corresponding vendor's advisory alert service.*
*Unify's product security team does not control or guarantee the currency, accuracy, or completeness of information found on the linked, external sites. If you need additional assistance, please contact your sales or services representative at Unify.*

## Affected Products

**Vulnerable:**
The following products are affected by CVE-2014-0160.

**1. Vulnerable with medium risk:**

- **OpenStage Cloud Diagnostic Data Collector** (Cloud-DDC):
  - **Solution available in hotfix V1 R4.0.1 (release date 2014-04-16)**
  - Attackers may have read the private key of the Cloud-DDC web server's TLS certificate as well as disclosed Cloud-DDC user passwords and/or the phone (OpenStage) admin passwords or other sensitive data being used in the Cloud-DDC session and sent to/from the individual phones.
- **OpenScape Voice Trace Manager** (OSV TM):
  - **Solution available in version V7 R0.8.0 (release date 2014-05-01)**
  - Only versions V7 R0.0.0 and above are vulnerable; they are affected only if the remote web access interface was/is enabled. An interim solution is to disable the remote web access; see chapter "Recommended Actions" for details.
- Partner product: **ASC Telecom - EVOip Voice Recording System:**
  - **Solution available in hotfix version V10 R0.17.0-19 (release date 2014-05-02)**
  - An interim solution is to disable access to the Web interface; see chapter "Recommended Actions" for details.
  - **Important note:** when the hotfix is applied, all recording services are stopped (and restarted automatically after the software update). Customers who need to record all calls for regulatory purposes should schedule the update outside the normal working hours.

**2. Vulnerable with low risk:**

- **OpenStage Diagnostic Data Collector (DDC):**
  - **Solution available in hotfix V4 R3.10.1 (release date 2014-04-16)**
  - The risk is rated low (CVSS v2 Base Score 2.6) and not seen as relevant in practice.
    This is a client-only use of a vulnerable implementation of openSSL. Attackers need to pretend to be a legitimate phone to disclose the admin password or other sensitive data that a legitimate DDC user may use in a session with a phone. This is similar to a Man-in-the-Middle (MitM) attack, where the attacker can already achieve the same, even without exploiting CVE-2014-0160.
    Thus, the vulnerability by itself does not cause additional risk.
- **SecM and Mpci libraries** (used by third-party applications to connect with the Assistant resp. the RMX/AMO interface on HiPath/OpenScape 4000):
  - **Solution available for SecM library in hotfix V7 R0.0.1 (release date 2014-04-16)**
  - **Solution available for Mpci library in version 1.6 (release date 2014-04-29)**
  - 3rd party applications that use these libraries can request them through their regular support channels at Unify. Furthermore, the new versions are also delivered as part of the next scheduled releases of HiPath 4000 Assistant (current plan dates and versions: E05/2014: V7 R0.14.5, M06/2014: V6 R2.42.4).
  - The risk is rated low (CVSS v2 Base Score 2.6).
    This is a client-only use of a vulnerable implementation of openSSL; the individual risk depends on the use of the libraries in the application itself. Typically, attackers would need to pretend to be a legitimate HiPath 4000 to disclose authentication data or other sensitive data that an application user may use in a session with HiPath 4000 Assistant (SecM) or HiPath 4000 RMX/AMO interface (Mpci). This is similar to a Man-in-the-Middle (MitM) attack, where the attacker can already achieve the same, even without specifically exploiting CVE-2014-0160.
    Thus, the vulnerability by itself does not cause additional risk.
- **HiPath Expert Access** ("ComWin" Service tool): relies on the vulnerable SecM library (but not on a vulnerable Mpci library)
  - **Solution available in version V5 R0.119.0 (release date 2014-04-16)**
  - The risk is rated low (CVSS v2 Base Score 2.6) and not seen as relevant in practice.
    This is a client-only use of a vulnerable implementation of openSSL. Attackers need to pretend to be a legitimate HiPath 4000 to disclose authentication data or other sensitive data that a legitimate ComWin user may use in a session with HiPath 4000 Assistant. This is similar to a Man-in-the-Middle (MitM) attack, where the attacker can already achieve the same, even without exploiting CVE-2014-0160.
    Thus, the vulnerability by itself does not cause additional risk.
- **Remote Test Tool HPT** (Husim Phone Tester):
  - **Solution available in version V2.0 R2.0.0 (release date 2014-04-17)**
  - Only versions V2.0 R1.2.x are affected
  - The risk is rated low (CVSS v2 Base Score 2.6) and not seen as relevant in practice.
    This is a client-only use of a vulnerable implementation of openSSL. Attackers need to pretend to be a legitimate phone to disclose the admin password or other sensitive data that a legitimate HPT user may use in a session with a phone. This is similar to a Man-in-the-Middle (MitM) attack, where the attacker can already achieve the same, even without exploiting CVE-2014-0160.
  - Note also that HPT will reach its scheduled end-of-life date very soon (the plan date is end of June 2014); the preferred solution is therefore to switch to the Java version (jHPT), which is not vulnerable.

**Not vulnerable:**
The following products are confirmed as not being affected by the Heartbleed vulnerability:

**Unified Communications:**

- **Voice Platforms:**
  - OpenScape Voice
  - HiPath 4000 V6 / OpenScape 4000 V7
  - OpenScape Branch
  - OpenScape Session Border Controller (SBC)
  - RG8700 and RG8300/RG8350a Gateways
  - OpenScape Alarm Response (OScAR) and HiPath DAKS
- **Applications:**
  - OpenScape UC Applications (incl. Common Management Portal, Facade Server, Media Server)
  - OpenScape Web Collaboration
  - OpenScape Xpressions
  - OpenScape ComAssistant
  - HiPath CAP
- **Phones and Clients:**
  - OpenStage and OpenScape Desk Phone IP VoIP phones
  - OpenStage WL3 and WL3 Plus, Wireless Services Gateway (WSG) and WinPDM
  - HiPath Cordless IP
  - OpenScape Mobile
  - OpenScape Personal Edition
  - AC-Win IP, BLF-Win
- **Management Applications:**
  - OpenScape Identity and Lifecycle Assistant (OS ILA)
    *Please note the details regarding OS ILA in the chapter "Recommended Actions"*
  - OpenScape License Management (CLM, CLC, CLA)
  - HiPath/OpenScape 4000 Manager
  - OpenScape Deployment Service (DLS)
  - OpenScape Accounting Management, User Management, Fault Management, QoS Management
  - HiPath Accounting Management
  - HiPath Directory Service for Windows (DS-Win)

**Contact Center:**

- OpenScape Contact Center Agile and Enterprise (OSCC)
- OpenScape Call Director SIP Server
- OpenScape Contact Center Extensions (OSCC-E - Concierge)
- OpenScape Contact Center Campaign Director

**Small and Medium Business:**

- OpenScape Business
  - Note that version V1 R3 is vulnerable (but is not yet released - all field trial customers have been informed directly with appropriate solution details)
- OpenScape Office
- HiPath 3000
- Associated clients (e.g. UC clients) and applications (e.g. TeleData Office)

**Financial Industry:**

- OpenScape Xpert

**HealthCare Industry:**

- OpenScape Health Station HiMed
- HiPath Healthcare Solution HiMed Nurse Call IP
- HiPath Healthcare Solution HiCall

**Managed Services, Maintenance and Support:**

- **Service and Diagnosis systems and tools:**
  - SESAP
  - jHPT and HPT (except HPT versions V2 R1.2.x - see above)
  - IP-Services
- **Remote and Managed Services**:
  - Smart Services Delivery Platform (SSDP), RSPssh
  - Proactive Support: Zenoss Customer Services Application (CSA) and Customer Gateway (CGW); OpenScape Backup and Recovery Services
  - Also, TLS-protected access to the RSP (Remote Service Platform - SIRA) itself was not vulnerable at any time.

**Partner Products:**

- Mediatrix VoIP Gateways (all versions released with Unify solutions)
- Oracle (ACME) Session Border Controller
- ASC Telecom: EvoLite Voice Recording System
- Verint QM Voice Recording (all versions released with Unify solutions)
- Genesys Products (all versions released with Unify solutions)
- Interalia: XMU+ and SBX Messaging Platforms

**End of life products:**
Unless specified explicitly, all versions of the listed products are included that are in the phase between general availability (GA) and end of life (EOL). Products or product versions that are beyond EOL are typically not considered in security advisories.
Informal note: optiPoint SIP and HFA phones, and HiPath 4000 V5 (all beyond EOL) are not vulnerable to CVE-2014-0160.
Note that the vulnerability did not exist before 2012-03-14 - which is the release date of the first vulnerable version of openSSL (1.0.1). Therefore, a product where the software was not changed since that time can be considered as not vulnerable.

## Recommended Actions

No activities are necessary for products that are confirmed as not vulnerable.

Regarding vulnerable products: wherever possible, limit the network access to authorized systems or user workstations only. Upgrade to appropriate fix releases as soon as they are available.

After the software update is completed:

- replace all TLS certificates that have been imported and activated on the vulnerable systems
- advise all users or administrators to change their passwords used at the TLS (Webbased Management) interfaces of the vulnerable products

**Recommended additional product-specific actions:**

**OpenScape Cloud Diagnostic Data Collector (Cloud-DDC)**:
After update to the new version, regenerate new individual admin passwords for all VoIP phones that were accessed by using the Cloud-DDC's web interface.

**OpenScape Voice Trace Manager (OSV-TM)**:
Until the fix release is available and installed, customers should disable the remote web access to OSV-TM as follows:

- Use Remote Desktop or access the OSV-TM server using the Windows credentials
- Run the "OSV-TM Security Manager" utility (accessible from the Start->OSV-TM->Security menu)
- Uncheck the "FADE Remote Access" checkbox and press "Save"

OSV-TM continues to work normal, collecting and analyzing trace files.
If users need to access FADE then they will need first to remote desktop to the server by using the Windows credentials and run FADE locally.

If there is a suspicion that the server was attacked, then the FADE userid/passwords should be changed to new sets via the FADE-->Administration-->Manage_users screen.
Once the new version of OSV-TM is available and the system is upgraded: if remote web access is desired by the customer, then they can re-enable FADE remote access by checking the box "FADE Remote Access" in the OSV-TM Security Manager.

**ASC Telecom - EVOip Voice Recording System:**
*EVOip 10* is only affected at the Web interface (https/TLS - default ports 443 and 8443) which serves both for administration *ASC DataManager* ("Config client") and end-user applications *WEBplay/INSTANT WEBplay* ("search-and-replay").
All functions offered at the Web interface are also available via the corresponding Windows clients or locally on the system, where this vulnerability does not apply; an interim countermeasure, until the fix release is available and installed on customer site is therefore:

- to disable the web-based interface on *EVOip 10*
- Change all users' logon passwords
- Access the *EVOip 10* via the *POWERplay/INSTANTplay* (Windows clients) or locally on the system, until the fix is installed
- Before reactivating the Web interface again, and in case a customized web server certificate was installed: replace the certificate incl. its private key by a new one

**OpenScape Identity and Lifecycle Assistant (OS ILA):**

- OS ILA relies on the DirX Directory database, where a patch was made available by the vendor (ATOS). This patch is not relevant to installations of standard OS ILA. Nevertheless, the patch can also be installed on installations of OS ILA.
- If the DirX Directory Phonebook application is installed on a separate server, the secured connection (LDAPS protocol) between DirX and a Phonebook server is affected; we recommend to install the associated patch for DirX Directory (according to the vendor's information) and review/change the affected login credentials afterwards.
- For details refer to information provided by ATOS at https://iam-support.it-solutions.atos.net/
  Note: this link requires registration at the ATOS partner and customer support portal; as a customer of Unify / OS ILA you can register; please contact your Sales or Services representative at Unify if you need support.
  Unify-related summary of the current information regarding DirX Directory:
  - V8.1 is not affected, this version relies on an older OpenSSL version
  - V8.2 is affected, a patch is available
  - V8.3 is not relevant, as not used by OS ILA

## References

External links:

- Mitre: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-0160
- NVD: http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2014-0160
- openSSL: https://www.openssl.org/news/secadv_20140407.txt
- Description of the Heartbleed bug: http://heartbleed.com/

Unify:

- Public link to this advisory: Unify Security Advisory OBSO-1404-02
- Appendix OBSO-1404-02-A (Information regarding Third-Party Products)
- Press releases: English, German

## Revision History

2014-04-11: Initial release
2014-04-15: Update 01:

- Included statements for additional products and libraries
- Errata: OpenScape Accounting is **not** affected
- HiPath/OpenScape 4000 and 4000 Manager are not affected.
- Added specific mitigation information for various products, incl. separation between medium and low risk

2014-04-18: Update 02:

- Added release information for Cloud-DDC and DDC, SecM library, HiPath Expert Access and HPT
- Included statements for many additional products
- Added notes regarding third-party products and end-of-life products and additional references

2014-04-18: Update 03:

- Included status information and interim solution for OpenScape Voice Trace Manager

2014-04-23: Update 04:

- Included statements for additional products: OS ILA, OpenScape Backup and Recovery
- Rearranged list of not affected products for better readability

2014-04-25: Update 05:

- Updated status information for OpenScape Voice Trace Manager
- Included status information and interim solution for ASC EVOip

2014-05-02: Update 06:

- Added release information for OpenScape Voice Trace Manager, ASC EVOip and Mpci library
- Added important note when applying the update of ASC EVOip
- Minor adaptations in wording

---

Advisory ID: OBSO-1404-02 (a=79), 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
© Unify Software and Solutions GmbH & Co. KG 2014
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.