Security Advisory Report - OBSO-1601-01

OpenSSH Client Information Leak Vulnerability (CVE-2016-0777)

Creation Date: 2016-01-26
Last Update: 2016-04-04

Summary

On January 14, 2016 a vulnerability in the OpenSSH client implementation was reported that could potentially allow malicious SSH servers to read portions of data of an OpenSSH client, including the leakage of private keys or passwords as used by the client.

The issue is caused by vulnerable implementation of an undocumented experimental roaming feature in the OpenSSH client, as documented in CVE-2016-0777 and in the Qualys Security Advisory.

The risk is rated **low** for some Unify products, most Unify products are not affected by this vulnerability.
This advisory lists the affected versions of Unify products and associated recommended actions.
It also provides a note regarding other OpenSSH vulnerabilities that were disclosed on the same day.

Vulnerability Details

The OpenSSH client code between version 5.4 and version 7.1 contains experimental support for resuming SSH-connections (roaming). The matching server code has never been shipped, but the client code was enabled by default and contains two flaws:

1. CVE-2016-0777 - Information Leak:
OpenSSH client could be tricked by a malicious server into leaking client memory to the server, including private client user keys.
Some Unify products are impacted as described in the section "Affected Products" below.

CVSSv3 scores for Unify Products:

- Base Score: 3.1 (Low)
- Temporal Score 2.9 (Low)
- CVSS v3 Vector (CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:N/A:N/E:P/RL:W/RC:C)

2. CVE-2016-0778 - Buffer Overflow:
Two API functions may overflow in some scenarios after a successful reconnection which may lead to remote code execution in certain non-default configurations.
Unify products are not affected as their default configuration of the OpenSSH client prevents from corresponding buffer overflows to occur.

Additional note about OpenSSH vulnerabilities:
Further vulnerabilities were disclosed on January 14 in the context of the new OpenSSH release 7.1p2 (release notes):

- CVE-2016-1907 - Out of bound read access in the packet handling code; fixed in OpenSSH 7.1p2
- CVE-2016-1908 - Unexpected fallback to trusted X11 forwarding; this issue is still unfixed in the latest version of OpenSSH, therefore it has been withdrawn from the OpenSSH release notes.

Unify products are not affected by these vulnerabilities.

Affected Products

Products confirmed as vulnerable:

- OpenScape Branch and OpenScape SBC
- OpenScape 4000 Assistant V7 R2 (but not in V7 R1 or V6 R2)
- OpenScape 4000 Manager (any version, but only when running on SUSE Linux Enterprise Server 11 SP3 or later)

Products (Linux-based devices, appliances or applications) confirmed as not vulnerable:

- OpenScape Voice
- OpenScape 4000 V7 / HiPath 4000 V6 (Platform, Softgate, HG35xx Gateways, CSTA)
- OpenScape 4000 Assistant V7 R1, HiPath 4000 Assistant V6 R2
- OpenScape Business, OpenScape Office
- OpenStage / OpenScape Desk Phone IP SIP/HFA

- OpenScape Contact Center Call Director SIP Service (CDSS)
- OpenScape UC Application
- OpenScape Common Management Platform (CMP)
- OpenScape Alarm Response (OScAR) Eco and Pro
- HiPath Cordless IP

Recommended Actions

1. OpenScape Branch and OpenScape SBC:
OpenScape Branch and OpenScape SBC use the OpenSSH client to download SW images, upload traces or upload CDR logs from/to remote SSH/SFTP servers. If different SSH/SFTP servers are configured and one of them runs a maliciously modified OpenSSH server (i.e. compromised by an attacker), the attacker could potentially read further credentials (passwords/private keys) as configured in the Branch or SBC appliance to access other SSH/SFTP servers. This may help to launch further attacks against these other SSH/SFTP servers or the OpenScape solution in general.

Fix releases:

- OpenScape Branch and OpenScape SBC: Upgrade to V8 R1.6.0 (INF-16-000117/INF-16-000118, release date: 2016-02-04) or any later version (Note: V8 R1.7.0 or later is recommended, see OBSO-1602-02)

Mitigation measures:

- Logon as superuser (root) on the OpenScape Branch or SBC appliance and modify the file /etc/ssh/ssh_config as described below (*).
  Note that this change is not persistent and has to be repeated after every restart of the appliance.
- Review the list of configured servers that OpenScape Branch or SBC are accessing via the SFTP protocol: File servers for SW download, servers where the trace information is uploaded (typically this is OpenScape Voice Trace Manager), billing servers where CDR data is uploaded.
  Harden the servers to prevent from illegitimate access. On suspicion of illegal access to any server in the past, change all access credentials and update the configuration in OpenScape Branch and SBC accordingly.

2. OpenScape 4000 Assistant V7 R2 and OpenScape Manager (running on SUSE Linux Enterprise Server SP3/SP4):
OpenScape 4000 Assistant and Manager use the OpenSSH client for backup/restore (HBR component) to a remote server, and for the Smart Switch Over (SSO) feature to connect multiple instances of OpenScape 4000 Manager in a high availability solution.
If one of the SSH/SFTP servers runs a maliciously modified OpenSSH server (i.e. compromised by an attacker), the attacker could potentially read further credentials (passwords/private keys) as configured in OpenScape 4000 Assistant or Manager, and access other servers. This may help to launch further attacks against these other SSH/SFTP servers or the OpenScape 4000 Manager.
An actual risk would be seen only, if

- Multiple OpenScape 4000 systems have already been upgraded to V7 R2 (initial GA release was 2015-12-17), and
- HBR is configured on these systems to potentially untrusted remote SSH/SFTP servers, and
- SSO is enabled and running on SLES 11 SP3/SP4-based OpenScape 4000 Manager servers.

Fix releases:

- **OpenScape 4000 Assistant V7 R2: Upgrade to V7 R2.20.2 (HF004428, release date: 2016-04-04) or any later version**
  (Note that V7 R2.20.1 (HF004414) already contained the fix, but its release on 2016-03-28 was withdrawn due to another issue, not related with CVE-2016-0777).
- OpenScape 4000 Manager: Apply the patch as provided by SUSE Linux Enterprise Server 11 SP3 or SP4 (CVE-2016-0777 - release date: 2016-01-14)

Mitigation Measures:

- Logon via SSH as administrator (engr) on the OpenScape 4000 Assistant or Manager and modify the file /etc/ssh/ssh_config as described below (*).
- On OpenScape 4000 Manager servers, apply the patch as provided by SUSE Linux Enterprise Server 11 SP3 or SP4 (CVE-2016-0777 - release date: 2016-01-14).
- Review the list of configured servers that are used for the backup/restore (HBR) feature.
  Harden the servers to prevent from illegitimate access. On suspicion of illegal access to any server in the past, change all access credentials and update the configuration in OpenScape 4000 Assistant and Manager accordingly.
- Install the product update for OpenScape 4000 Assistant, once available.

Note: OpenSSH client is also used internally in OpenScape 4000 (e.g. for SSH maintenance access to SoftGate or HG35xx Gateways). However, no practical exploitability could be identified (beyond the scenario described for OpenScape 4000 Assistant and Manager above).

(*) Modification of the OpenSSH client configuration file:

Logon as superuser (root) on the OpenScape Branch or SBC appliance and modify the file ***/etc/ssh/ssh_config*** as follows. Look for the line:

*Host **

e.g. the relevant section may look like:

*Host **
 # ForwardAgent no
 # ForwardX11 no

Add a line "*UseRoaming no*" as in the example below and save the file:

*Host **
UseRoaming no
 # ForwardAgent no
 # ForwardX11 no

References

- Qualys Security Advisory "Roaming through the OpenSSH client: CVE-2016-0777 and CVE-2016-0778"
- NIST/NVD vulnerability entries: CVE-2016-0777, CVE-2016-0778
- CERT/CC vulnerability entry VU#456088
- FIRST: Common Vulnerability Scoring System (CVSS), V3

Vendor release/patch information:

- OpenSSH: Release notes Version 7.1p2
- SUSE Linux Enterprise Server: CVE-2016-0777

Revision History

2016-01-26: Initial release
2016-02-04: Update 01

- Fix release available for OpenScape Branch and OpenScape SBC

2016-02-25: Update 02

- Error correction: release version for OpenScape Branch and SBC is V8 R1.6.0 (not V8 R1.8.0); added note regarding upcoming release of V8 R1.7.0

2016-03-28: Update 03

- Fix release available for OpenScape 4000 Assistant V7 R2

2016-04-04: Update 04

- Updated information regarding the fix release for OpenScape 4000 Assistant V7 R2
  (Use V7 R2.20.2 instead of V7 R2.20.1)

Advisory ID: OBSO-1601-01 (a=130), 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