Security Advisory Report - OBSO-1512-03

OpenSSH Login Handling Security Bypass Vulnerability (CVE-2015-5600)

Creation Date: 2015-12-30
Last Update: 2016-10-25

Summary

The OpenSSH component as included in various Linux-based appliance products of Unify contains a vulnerability that could allow an unauthenticated, remote attacker to bypass the limit of invalid Secure Shell (ssh) login attempts. This could facilitate password guessing attacks against the operating system level accounts.

The risk is rated **medium**.

The issue is caused by a flaw in the sshd daemon of OpenSSH as documented in CVE-2015-5600 and in the OpenSSH V7.0 Release Note.

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 in 2015.

Vulnerability Details

The OpenSSH sshd daemon does not check the list of keyboard-interactive authentication methods for duplicates. A remote attacker could use this flaw to bypass the "MaxAuthTries" limit (a sshd configuration parameter that limits the number of allowed invalid logon attempts in a single ssh connection, before this connection is closed).

In Unify products "MaxAuthTries" is configured between 3 and 6. The flaw could allow a remote attacker to try thousands of different passwords in a single connection, thus making it easier to perform password guessing attacks.
The maximum number of password guesses is limited by the network connection and speed, and by the "LoginGraceTime" (which is configured between 30 seconds and 2 minutes in Unify products).

Mitre has assigned CVE-2015-5600 to this issue in OpenSSH. Further information is available in the OpenSSH 7.0 Release Note.

CVSSv3 scores for Unify Products:

- Base Score: 5.6 (Medium)
- Temporal Score 5.5 (Medium)
- CVSS v3 Vector (CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:L/I:L/A:L/E:F/RL:U/RC:C)

Additional note about OpenSSH vulnerabilities:
In 2015 further vulnerabilities were disclosed in the context of new OpenSSH versions as follows: Version 6.9 (CVE-2015-5352), version 7.0 (CVE-2015-6563, CVE-2015-6564, CVE-2015-6565) and version 7.1 (no CVE ID).
They are summarized at the OpenSSH Security Advisory page (http://www.openssh.com/security.html).
Unify products are not affected by these vulnerabilities, except for CVE-2015-6563, which is rated as low risk issue. The same recommended actions and product fix releases apply as described below for CVE-2015-5600.

Affected Products

Products confirmed as vulnerable:

- OpenScape Voice, OpenScape Branch, OpenScape SBC
- OpenScape 4000 V7 R1 and V6 R2: Platform, Softgate, Assistant, CSTA
- OpenScape Contact Center Call Director SIP Service (CDSS)

Products confirmed as vulnerable, but with low risk only:

- OpenScape Business and OpenScape Office
  (SSH access is disabled by default and may only be enabled temporarily for exceptional administrative tasks)

Products confirmed as not vulnerable (Linux-based appliances and embedded devices)**:**

- OpenScape 4000 V7 R2: Platform, Softgate, Assistant, CSTA
- OpenScape 4000, all versions: HG Gateways
- OpenStage / OpenScape Desk Phone IP SIP and HFA
- OpenStage Xpert
- OpenScape Alarm Response (OScAR) Eco and Pro
- HiPath Cordless IP

Recommended Actions

Fix Releases:

- OpenScape 4000 V7: Update to V7 R2.23.0 (release date: 2015-12-17) or any later version
- OpenScape Branch and OpenScape SBC: Update 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)
- OpenScape Voice V8 R1: Install Server Image V8 R1.44.0_04 (V8.00.01.ALL.08_PS0044, INF-16-000123, release date: 2016-03-23) or any later version
- OpenScape Voice V7 R1: Install Server Image V7 R1.**51**.0_04 (V7.00.01.ALL.07_PS00**51**.E04, INF-16-000077, release date: 2016-04-22) or any later version
- OpenScape Voice V9: Install Server Image V9 R0.8.3_01 (V9.00.01.ALL.12_PS0008.E03, INF-16-000200, release date: 2016-04-28)
- **OpenScape Contact Center Call Director SIP Service (CDSS): Update to V9 R0.2.0 (INF-17-000034, release date: 2016-10-21) or any later version**

Mitigation Measures:
The following settings are recommended as general best-practice security hardening in the customer's network - regardless if a fix for this particular issue in the affected Unify product(s) is installed or not.

- Apply suitable network configuration measures to restrict the access to the SSH server port (**22/tcp**) of Unify appliances to authorized systems and users only.
- If network security solutions (such as IDS, IPS, SIEM or similar) are in place: monitor network traffic to identify/prevent potentially suspicious ssh traffic.
- Configure long (e.g. more than 10 characters), strong and individual passwords for the operating system accounts provided by the Unify appliance to limit the risk of successful brute-force attempts. For information about the relevant system accounts and further recommendations refer to the individual product's Security Checklist.

Note:
For Linux-based Unify server applications follow the recommendations provided by the operating system vendor. The following vulnerability and patch information is available:

- SUSE Linux Enterprise Server: CVE-2015-5600
  Risk: high
  Relevant for:
  - OpenScape UC Application (Frontend, Backend, Facade, Media and OpenFire servers) and Common Management Platform
  - OpenScape Voice Survival Authority
  - OpenScape 4000 Manager
  - OpenScape Business S and UC Booster Server, OpenScape Office LX/HX
- Debian Linux: CVE-2015-5600
  Risk: low (not vulnerable in default OpenSSH configuration)
  Relevant for: OpenScape Xpert MLC

References

- NIST/NVD vulnerability entry: CVE-2015-5600
- OpenSSH:
  - OpenSSH 7.0 Release Note
  - OpenSSH Security Advisories: http://www.openssh.com/security.html
- FIRST: Common Vulnerability Scoring System (CVSS), V3

Information for Application Server Operating Systems:

- SUSE Linux Enterprise Server: CVE-2015-5600
- Debian Linux: CVE-2015-5600

Revision History

2015-12-30: 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

2016-03-25: Update 03

- Fix release available for OpenScape Voice V8 R1

2016-08-08: Update 04

- Fix releases available for OpenScape Voice V7 R1 and V9

2016-10-25: Update 05

- Error correction: release version for OpenScape Voice V7 R1 was V7 R1.51.0_04 (not V7 R1.54.0_04)
- Fix release available for OpenScape Contact Center CDSS

Advisory ID: OBSO-1512-03 (a=127), 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

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.