Security Advisory Report - OBSO-1503-01

OpenScape SBC V8 - SIP Authentication Bypass Vulnerability (CVE-2015-2057)

Creation Date: 2015-03-03
Last Update: 2015-03-24

Summary

An authentication bypass vulnerability in the SIP (Session Initiation Protocol) interface of OpenScape Session Border Controller (SBC) V8 may - in certain configurations - allow remote attackers, within a limited time window, to perform illegitimate VoIP (Voice over IP) calls .

The risk is rated **high.**
Customers who determine its applicability to their environment should apply the mitigation measures listed below at the earliest opportunity.
They provide effective prevention from the potential attacks described in this advisory, thereby **reducing the risk to none**.

Vulnerability Details

OpenScape SBC V8 contains an authentication bypass vulnerability (as defined in the Common Weakness Enumeration CWE-592) in the SIP (Session Initiation Protocol) interface.
This vulnerability could be leveraged in certain configurations where OpenScape SBC V8 as a trusted endpoint is serving remote subscribers (e.g. teleworkers) that are configured as trusted. Remote unauthenticated attackers could send a sequence of (unsuccessful) SIP REGISTER messages that are, within a limited time window of ~5 minutes, followed by (successful) SIP INVITE messages.
The sequence may bypass digest authentication of the INVITE message by the SIP server (e.g. OpenScape Voice) located behind the SBC. This may allow illegitimate VoIP calls, potentially leading to toll fraud attacks.

CVSS scores:

- Base Score: 9.0
- Temporal Score 8.5
- CVSS v2 Vector (AV:N/AC:L/Au:N/C:P/I:C/A:P/E:H/RL:W/RC:C)

Mitre (cve.mitre.org) has assigned the id **CVE-2015-2057** to this issue.
A correction for OpenScape SBC V8 is in work, but not yet released. However, a solution is already available: affected customers should apply the mitigation measures listed below at the earliest opportunity.

Affected Products

- OpenScape SBC V8 before V8 R0.28.0

OpenScape SBC V7 and earlier versions are not affected. Note that the measures outlined in the section below are valid and recommended for solutions with OpenScape SBC V7 and earlier versions as well.

Recommended Actions

1. Implement the following mitigation measures.
They protect against the potential attacks described in this advisory. The description is based on a typical setup OpenScape SBC <-> OpenScape Voice (OSV); analogous measures apply in case a different communication platform is used in conjunction with OpenScape SBC.

- On OpenScape Voice, enable Digest Authentication for all subscribers, and use individual and strong passwords
- Configure all SIP endpoint ports that serve remote subscribers as "untrusted"; in other words: exclude all mapped Session Border Controller addresses (IP + port-range) identifying static or dynamically registering remote subscribers from the OpenScape Voice trusted realm
- Set the RTP parameter Srx/Sip/AuthTraverseViaHdrs to value RtpFalse

For more details refer to chapters 3.4.7 - 3.4.11 of the OpenScape Voice Security Checklist:

- **V8: Issue 8, released 2015-03-24**
- **V7: Issue 12, released 2015-03-24**

or later document versions.

The following additional measures further contribute to protect against most of the known attack patterns:

- Use TLS (instead of TCP or UDP) as the SIP communication protocol on the SBC's WAN/Internet interface for remote subscribers and configure a different port than the default port 5061
- If TCP or UDP is used and cannot be changed to TLS: configure a different port than the default port 5060

For further information please see the latest Installation Guides and Security Checklists for OpenScape SBC and OpenScape Voice.

2. Update OpenScape SBC V8 to V8 R0.28.0 (release date: 2015-03-13) or higher.
Note that the measures outlined in 1. are still valid and recommended, even when a patched version of OpenScape SBC V8 is used.

References

Mitre:

- http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-2057
- CWE-592

Revision History

2015-03-03: Initial release
2015-03-13: Update 01

- Fix release for OpenScape SBC V8 available

2015-03-24: Update 02

- Informational update: New issues of the OpenScape Voice Security Checklist available (containing details for the recommended mitigation measures listed in this advisory)

Advisory ID: OBSO-1503-01 (a=103), 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.