Security Advisory Report - OBSO-1508-02

OpenStage 60 / OpenScape Desk Phone IP 55G - Local service exposure vulnerability (CVE-2015-5391)

Creation Date: 2015-08-13
Last Update: 2015-08-13

Summary

OpenStage 60 and OpenScape Desk Phone IP 55G (SIP and HFA) expose a local service to the network that that could allow a remote unauthenticated attacker to read data and execute commands on the phone in a limited environment and with limited privileges.

The risk is rated **medium**.

Vulnerability Details

OpenStage 60 and OpenScape Desk Phone IP 55G (both SIP and HFA) expose a local service on network ports 16842/tcp and 16843/tcp (as defined in the Common Weakness Enumeration CWE-402). A remote unauthenticated attacker located in the same network as the phone could access these ports to retrieve data and potentially execute code in the context of the phone's local blued daemon (part of the bluetooth service implementation).
Only the "high-end" device models are affected, "low-end" device models do not expose bluetooth services.

CVSSv2 scores:

- Base Score: 6.4
- Temporal Score 5.0
- CVSS v2 Vector (AV:N/AC:L/Au:N/C:P/I:P/A:N/E:POC/RL:OF/RC:C)

CVSSv3 scores:

- Base Score: 6.5
- Temporal Score 5.9
- CVSS v3 Vector (AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C)

Mitre (cve.mitre.org) has assigned the id CVE-2015-5391 to this issue.
This vulnerability was found internally during regular security tests in accordance with Unify's Baseline Security Policy.

Affected Products

- OpenStage 60 / OpenScape Desk Phone IP 55G SIP, from V3 R1.19.0 (release date 2012-04-27) through V3 R3.40.0
- OpenStage 80 / OpenScape Desk Phone IP 55G HFA, from V2 R1.5.2 (release date 2014-08-28) through V3 R0.23.1

Only high end phone models are affected, while low end models (OpenStage 15/20E/20/40 / Desk Phone IP 35G) are not.

Recommended Actions

Install the following product releases (or later versions) to resolve the vulnerability:

- OpenStage 60 / OpenScape Desk Phone 55G SIP: V3 R3.40.1 (release date: 2015-07-24)
- OpenStage 60 / OpenScape Desk Phone 55G HFA: V3 R0.23.3 (release date: 2015-08-13)
  Note that the correction is also available in V3 R0.23.2, but this version did not achieve GA (general availability)

Mitigation measures:
If applicable in the individual customer's network environment, configure firewalls and IDS/IPS/SIEM systems appropriately to detect or block IP traffic from/to the exposed ports 16842/tcp and 16843/tcp of OpenStage 60 / OpenScape Desk Phone IP 55G phones.

References

- NIST/NVD vulnerability entry for CVE-2015-5391
- CWE-402

Revision History

2015-08-13: Initial release

Advisory ID: OBSO-1508-02 (a=115), status: general 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 2015
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.