Security Advisory Report - OBSO-1510-01

OpenScape Xpressions - unauthorized external calls via guest access (CVE-2015-7693)

Creation Date: 2015-10-26
Last Update: 2016-05-13

Summary

In a certain (**non-default**) configuration, the voice mail application of OpenScape Xpressions performs authorization checks incorrectly, which may allow remote unauthenticated attackers to establish illegitimate long distance or international calls.
This is a vulnerability as defined in CWE-863.

The risk is rated **medium**, as the potential exploitability requires special (uncommon) configuration settings.
A hotfix release is available to address this issue in OpenScape Xpressions V7 R1.
Furthermore the advisory provides hints to determine whether existing, unpatched installations may be vulnerable or not.

Vulnerability Details

In certain configuration settings, Phonemail in Xpressions V7 R1 allows to transfer calls to external parties **through the guest access** despite of the recommended hardening setting "-disabletransferout" (and "-notodr").

This may allow a remote unauthenticated attacker to establish long distance or international calls, if

- **Guest access is configured and enabled**
- NCOs (Number Configuration Objects) are inappropriately configured, so that external numbers are treated as internal extensions
- The parameter "MaxExtensionLength" is set to a high value (e.g. 12) that that is big enough for long external numbers

CVSS Scores:

- CVSSv2: Base Score 7.1, Temporal Score 6.2
  (AV:N/AC:M/Au:N/C:N/I:C/A:N/E:H/RL:OF/RC:C)
- CVSSv3: Base Score 5.9, Temporal Score 5.7
  (CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:H/A:N/E:H/RL:O/RC:C)

Affected Products

- OpenScape Xpressions V7 R1, all versions **before V7 R1.5.1**

Recommended Actions

Install version V7 R1.5.1 (release date: 2016-04-15) or any later version to resolve the vulnerability.

A private hotfix is available for earlier versions as follows:

- Hotfix HF004277 for OpenScape Xpressions V7 R1.5.0 ("Phonemail-811FR5-18495", GA release date: 2015-10-30), or
- Hotfix HF004285 for OpenScape Xpressions V7 R1.4.1 ("Phonemail-811FR4-18516", GA release date: 2015-10-30)

The hotfixes prevent external calls through the guest access, if the hardening setting "-disabletransferout" (and "-notodr") is enabled.

Mitigation recommendations for unpatched systems:

- On unpatched systems, review the current configuration settings, esp. review the NCO settings and reduce "MaxExtensionLength" to a number appropriate to your specific environment (e.g. 4 or 5)
- If applicable to your environment, remove the SYS_INTERNAL privilege from the user SYSTEM. This prevents the exploitability of the vulnerability completely.

References

- NIST/NVD vulnerability entry for CVE-2015-7693
- CWE-863

Revision History

2015-10-26: Initial release
2015-10-30: Update 01

- Added Hotfix information for OpenScape Xpressions V7 R1.4.1 and updated information for V7 R1.5.0 to reflect General Availability of both Hotfixes
- Clarification that the vulnerability existed when using the guest access and what is solved by the hotfix

2016-05-13: Update 02

- The fix is included in OpenScape Xpressions V7 R1.5.1 and any later version, without requiring a private hotfix.

Advisory ID: OBSO-1510-01 (a=120), 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.