UNIFY

Security Advisory Report - OBSO-1610-01

OpenScape Xpressions - Information Exposure Vulnerability Through HTTP GET Method at Web Assistant Interface

Creation Date: 2016-10-18
Last Update: 2016-10-18

Summary

The Web Assistant interface (WebApl) of OpenScape Xpressions before V7 R1.5.2 leaks sensitive session information through the use of the HTTP GET method.

The risk is rated **medium**.

Vulnerability Details

The Web Assistant uses the HTTP GET method to submit session keys, which are transmitted within the query string of the requested URL. As these URLs may be logged in various locations (such as the user's browser, the web server, or any forward or reverse proxy servers in between), it may be captured by an attacker.
This is a vulnerability as defined in CWE-598.

CVSSv3 Scores:

- Base Score: 5.4 (Medium)
- Temporal Score: 4.9 (Medium)
- Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C

Affected Products

- OpenScape Xpressions V7 R1, all versions before V7 R1.5.2

Recommended Actions

Update OpenScape Xpressions to V7 R1.5.2 (release date 2016-05-11) or any later version (current latest version is V7 R1.5.6, release date 2016-10-08).

A mitigation or solution for earlier versions is not available.

References

- Mitre: CWE-598: Information Exposure Through Query Strings in GET Request
- FIRST: Common Vulnerability Scoring System (CVSS), V3

Revision History

2016-10-18: Initial release

---

are subject to change without notice.