Security Advisory Report - OBSO-2107-01

Local privilege escalation vulnerability within Atos Unify OpenScape 4000 Assistant and Atos Unify OpenScape 4000 Manager

Release Date:	2021-07-01 15:57:26
Last Update:	2022-04-01 17:23:31

Summary

Atos Unify OpenScape 4000 Assistant and Atos Unify OpenScape 4000 Manager versions 10 and 8 are affected by several local privilege escalation vulnerabilities. If the vulnerabilities are successfully exploited, system accounts with low privileges on OpenScape 4000 Assistant and Manager may be used to run arbitrary command or escalate privileges to root. Refer to the Details for more information.

The vulnerability is rated medium.

Details

In order to exploit the vulnerability local access to the system is required and the affected system accounts need to be compromised. Attack vectors that would allow remote exploiting are not known at the time of the release of the Security Advisory. For OpenScape 4000 Manager compromise of a lower privileged local administration account is considered an additional attack vector.

While functional exploits are available for the local exploitation of the vulnerabilities, a remote exploitation requires an additional attack vector that has not been demonstrated so far. A local exploitation on OpenScape 4000 Manager requires a user account and some form of user interaction in order to gain low privileged access.

The vulnerability is rated medium with a CVSS base score of 7.0 and CVSS temporal score of 6.8
https://www.first.org/cvss/calculator/3.1#CVSS:3.1/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:F/RL:U/RC:C/CR:H/IR:H/AR:H/MAV:L/MAC:H/MPR:L/MUI:N/MS:U/MC:H/MI:H/MA:H

Affected Products

Products confirmed affected

OpenScape 4000 Assistant and OpenScape 4000 Manager versions V10 before version V10 R0.28.7 (available)

OpenScape 4000 Assistant and OpenScape 4000 Manager versions V8 before version V8 R2.22.16 (available)

Recommended Actions

Implement OpenScape 4000 Assistant/Manager Hotfix V10 R0.28.7 / V8 R2.22.16

General recommendations:

- Operate OpenScape 4000 Assistant and Manager within secured networks according to the recommendations of the Security Checklist
- Always implement the latest available patches and hotfixes

References

Change History

Version	Date	Description
1.2	05.01.2022	- Initial release and version up to V1.2
1.3	07.03.2022	- For V8 a fix is planned in V8 R2.22.1 for March 2022.
1.4	22.03.2022	- For V8 a fix is planned in **V8 R2.22.16** for March 2022.
1.5	01.04.2022	- For V8 fixed in V8 R2.22.16 (available)

Advisory: OBSO-2107-01, status: update release
Security Advisories are released as part of Atos Unify's Vulnerability Intelligence Process. For more information see https://www.unify.com/security/advisories.

Contact and Disclaimer

OpenScape Baseline Security Office
obso@atos.net

Otto-Hahn-Ring 6
D-81739 München
www.unify.com