Security Advisory Report - OBSO-2201-02

Directory Traversal vulnerability in Atos Unify OpenScape Xpressions

Release Date: 2022-01-24 16:17:33
Last Update: 2022-02-10 17:55:22

Summary

A Directory Traversal (or Path Traversal) vulnerability was discovered in Atos Unify Xpressions V7R1 FR5 HF40, which can be exploited to view the contents of arbitrary files on the local file system. An unauthenticated attacker might be able to obtain sensitive message contents, personal user data, and potentially compromise the underlying host.

The vulnerability exists due to improper validation of the URL path folders in HTTP requests, where an attacker may download arbitrary files by submitting a system file path with directory traversal character sequences.

It is strongly recommended to apply the WebApl-811FR5-20908 (XPR V7 R1 FR5 HF40 P909) hotfix as soon as possible.

The vulnerability is rated high severity.

Details

The vulnerability is rated high with a CVSS3.1 score of 7.5
CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N

Note:
The initial hotfix Webapl-811FR5-20902 (XPR V7 R1 FR5 HF40 P907) that has been provided has been incomplete

Affected Products

All versions of Atos Unify OpenScape Xpression V7 up to, and including Webapl-811FR5-20902 (XPR V7 R1 FR5 HF40 P907)

Recommended Actions

Apply hotfix WebApl-811FR5-20908 (XPR V7 R1 FR5 HF40 P909) as soon as possible.

References

Change History

Version	Date	Description
1.0	24.01.2022	- Initial release
1.1	10.02.2022	- Initial hotfix incomplete, new hotfix has been released

Advisory: OBSO-2201-02, status: general 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
© Unify Software and Solutions GmbH & Co. KG 2022
Otto-Hahn-Ring 6
D-81739 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.