

Security Advisory Report - OBSO-2211-01

OpenSSL V3 buffer overflow vulnerabilities (CVE-2022-3602 and CVE-2022-3786)

Release Date: 2022-11-08 14:11:29
Last Update: 2022-11-14 16:38:49
Version: 1.2

Summary

Two high priority vulnerabilities have been found in OpenSSL V3. Earlier versions OpenSSL 1.1.1 and 1.0.2 are not impacted by the vulnerabilities. Both vulnerabilities are related to a buffer overrun that can be triggered in X.509 certificate verification. CVE-2022-3602 potentially could cause a buffer overflow and allow remote code execution. However, the OpenSSL team states that :“many platforms implement stack overflow protections which would mitigate against the risk of remote code execution”. For details check [OpenSSL Security Advisory \[01 November 2022\]](#) .

We are currently analyzing the impact of the Atos Unify portfolio. At the current state of the evaluation, we have identified a few products that deploy a vulnerable version of OpenSSL.

The severity is rated medium.

Details

Based on the statement that OpenSSL has provided in [OpenSSL Security Advisory \[01 November 2022\]](#) :

- The primary risk is a denial of service condition on an affected interface
- The potential of remote code execution is reduced as "Many platforms implement stack overflow protections which would mitigate against the risk of remote code execution. The risk may be further mitigated based on stack layout for any given platform/compiler."
- "We are not aware of any working exploit that could lead to code execution, and we have no evidence of this issue being exploited as of the time of release of this advisory (November 1st 2022)."

Knowledge Base Article [KB000105083](#) has been issued in the Atos Unify Support Portal (registered users only) to provide additional information on the impact on affected Atos Unify products.

Affected Products

Product statements are related to product versions before End of Support (M44) is reached

Products confirmed affected

OpenScape UC Application V 10 version 10.4.8.2 and higher before 10.4.10.1

Affected sub product: OpenScape Media Server for UC/OSV 9.4.43.0 (V9.4.44.0 and higher are not affected)

Products confirmed not affected

Circuit

Unify Phone

Atos Unify OpenScape Business V3

Atos Unify OpenScape Voice (simplex deployments) V10

Atos Unify OpenScape 4000 V8 and V10 Platform

Atos Unify OpenScape 4000 V8 and V10 Assistant

Atos Unify OpenScape 4000 V8 and V10 CSTA

Atos Unify OpenScape 4000 V8 and V10 Loadware

Atos Unify OpenScape Voice (duplex deployments) V10

Atos Unify OpenScape Cordless IP V2

Atos Unify OpenScape First Response ESRP V9

Atos Unify OpenScape First Response BCF V10

Atos Unify OpenScape First Response ESAPP V1

Atos Unify OpenScape First Response PSS V1

Atos Unify OpenScape First Response MSBF V2

Atos Unify OpenScape Alarm Response Professional V4 and V5

Atos Unify Virtual Care Collaboration Service V1

Atos Unify OpenScape Xpert Clients V7

Atos Unify OpenScape Xpert MLC V7

Atos Unify OpenScape Xpert System Manager V7

Atos Unify OpenScape Branch V10

Atos Unify OpenScape SBC V10

Atos Unify OpenScape Contact Center V10,V11

Atos Unify OpenScape Contact Media Service V10,V11

Atos Unify OpenScape Fusion for Office V2

Atos Unify OpenScape Extensions for MS Outlook V2

Atos Unify OpenScape Fusion for Notes V2

Atos Unify OpenScape Web Collaboration V7

Atos Unify OpenScape Concierge V4

Atos Unify OpenScape Xpressions V7

Atos Unify OpenScape Personal Edition V7

Atos Unify OpenScape Media Server V9

Atos Unify OpenScape 4000 Manager V8 and V10

Atos Unify OpenScape Common Management Platform V10

Atos Unify OpenScape Composer V2

Atos Unify OpenScape Deployment Service V10

Atos Unify OpenScape Fault Management V11 and V12

Atos Unify OpenScape Accounting Management V4 and V5

Atos Unify OpenScape Voice Trace Manager V8

Atos Unify OpenScape Voice Survival Authority
Atos Unify OpenScape Desk Phones CP SIP
Atos Unify OpenScape Desk Phones CP HFA
Atos Unify OpenScape Desk Phones IP SIP V3
Atos Unify OpenScape Desk Phones IP HFA V3
Atos Unify OpenScape DECT Phone S5 and SL5
Atos Unify OpenScape DECT Phone R6, S6 and SL6
Atos Unify OpenScape WLAN Phone Wireless Service Gateway
AC Win SL V3
HiPath CAP V3.0
HiPath DS-Win V4
Atos Unify OpenScape Backup & Recovery Services
Atos Unify OpenScape Sesap V2
Atos Unify OpenScape License Management CLA/CLM

Products under investigation

Atos Unify OpenScape First Response NGLS V1
Atos Unify OpenScape WLAN Phone WL3 and WL4

Recommended Actions

Further information is provide in [KB000105083](#)

- Check whether affected products are publicly exposed
- Consider workaround instructions based on your individual risk analysis

References

- <https://www.openssl.org/news/secadv/20221101.txt>
- <https://nvd.nist.gov/vuln/detail/CVE-2022-3602>
- <https://github.com/NCSC-NL/OpenSSL-2022/blob/main/software/README.md>
- <https://dso.docker.com/cve/CVE-2022-3602>
- <https://security.alpinelinux.org/vuln/CVE-2022-3602>
- <https://www.suse.com/security/cve/CVE-2022-3602>
- <http://people.ubuntu.com/~ubuntu-security/cve/CVE-2022-3602>
- <https://security-tracker.debian.org/tracker/CVE-2022-3602>
- <https://www.docker.com/blog/security-advisory-critical-openssl-vulnerability/>

Version Change History

Version	Date	Description
1.0	08.11.2022	- Initial release
1.1	09.11.2022	- Corrected fix version OS UC V10 R4.10.1 - OpenScape Media Server for UC/OSV V9.4.44.0 and higher are not affected

Version	Date	Description
1.2	14.11.2022	- Fix for OpenScape UC V10 R4.10.1 is available

Advisory: OBSO-2211-01, 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

© 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.