

**PUBLIC - FOR EXTERNAL USE:** ([TLP: WHITE](#))

Subject to standard copyright rules, TLP:WHITE information may be distributed without restriction.

---

## Security Advisory Report - OBSO-2207-01

### OpenSSL Certificate Parsing Infinite Loop Remote DoS (CVE-2022-0778)

Status:	Update Release
Release Date:	2022-07-14 14:31:47
Last Update:	2023-11-07 07:58:54
Version:	1.8

#### Summary

OpenSSL contains an infinite loop in the BN\_mod\_sqrt() function in crypto/bn/bn\_sqrt.c that is triggered when parsing a specially crafted certificate with invalid explicit elliptic curve parameters. This may allow a remote attacker to cause a denial of service.

The vulnerability is tracked as [CVE-2022-0778](#), and affects OpenSSL versions 1.0.2 to 1.0.2zc, 1.1.1 to 1.1.1m, and 3.0 to 3.0.1.

The severity is rated medium to high.

#### Details

The BN\_mod\_sqrt() function, which computes a modular square root, contains a bug that can cause it to loop forever for non-prime moduli. Internally this function is used when parsing certificates that contain elliptic curve public keys in compressed form or explicit elliptic curve parameters with a base point encoded in compressed form. It is possible to trigger the infinite loop by crafting a certificate that has invalid explicit curve parameters. Since certificate parsing happens prior to verification of the certificate signature, any process that parses an externally supplied certificate may thus be subject to a denial of service attack. The infinite loop can also be reached when parsing crafted private keys as they can contain explicit elliptic curve parameters.

Thus vulnerable situations include:

- TLS clients consuming server certificates
- TLS servers consuming client certificates
- Hosting providers taking certificates or private keys from customers
- Certificate authorities parsing certification requests from subscribers
- Anything else which parses ASN.1 elliptic curve parameters

Also any other applications that use the BN\_mod\_sqrt() where the attacker can control the parameter values are vulnerable to this DoS issue. In the OpenSSL 1.0.2 version the public key is not parsed

during initial parsing of the certificate which makes it slightly harder to trigger the infinite loop. However any operation which requires the public key from the certificate will trigger the infinite loop. In particular the attacker can use a self-signed certificate to trigger the loop during verification of the certificate signature. This issue affects OpenSSL versions 1.0.2, 1.1.1 and 3.0. It was addressed in the releases of 1.1.1n and 3.0.2 on the 15th March 2022. Fixed in OpenSSL 3.0.2 (Affected 3.0.0,3.0.1). Fixed in OpenSSL 1.1.1n (Affected 1.1.1-1.1.1m). Fixed in OpenSSL 1.0.2zd (Affected 1.0.2-1.0.2zc).

Other components that use OpenSSL or components that are derived from OpenSSL are affected as well.

The CVSS3.1 base score is 7.5 (high)

[CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H](#)

The CVSS3.1 temporal score is 6.5 (medium)

[CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H/E:U/RL:O/RC:C](#)

We are currently not aware that the vulnerability is actively exploited.

## Affected Products

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

### Products confirmed affected

*Products with affected interfaces that may be publicly exposed (severity is considered high)*

#### Circuit

Atos Unify OpenScape Business V3 before V3R2

Atos Unify OpenScape Enterprise Express V10 (follow instructions for individual products)

Atos Unify OpenScape Voice (simplex deployments) V10 (follow instructions for individual products)

Atos Unify OpenScape 4000 V8 before V8R2.22.20 and V10 Loadware before V10R0.28.13

Atos Unify OpenScape Cordless IP V2 before V2R2.47.0

Atos Unify OpenScape First Response BCF V10 before V10 R10.0.0

Atos Unify Virtual Care Collaboration Service V1 before Sprint 90 (available)

Atos Unify OpenScape Branch V10 before V10R2.3.0

Atos Unify OpenScape SBC V10 before V10R2.4.0

Atos Unify OpenScape Contact Center Application Server V10 before V10R4.5.0 and V11R0.4.0

Atos Unify OpenScape Contact Center OpenMedia Connector V1 before V1R0.5.0

Atos Unify OpenScape Contact Media Service V10,V11 before V11R0.3.0

Atos Unify OpenScape Fusion for Office V1 and V2 before V2 R1.18.0 and V1 R8.32.0

Atos Unify OpenScape Fusion for Notes V1 and V2 V2 R1.18.0 and V1 R8.32.0

Atos Unify OpenScape Xpressions V7 before V7 R1.5.0 HF41 (available)

*Products with affected interfaces that are expected not to be publicly exposed (severity is considered*

*medium)*

Atos Unify OpenScape 4000 V8 and V10 Platform before V10 R0.28.8 and V8 R2.22.11  
 Atos Unify OpenScape 4000 V8 and V10 Assistant before V10 R0.28.11 and V8 R2.22.17  
 Atos Unify OpenScape 4000 V8 and V10 CSTA before V10 R0.28.9 and V8 R2.22.13  
 Atos Unify OpenScape Voice (duplex deployments) V10 before V10 R3.16.1  
 Atos Unify OpenScape Contact Center Server V10 before V10R4.8 and V11R1.1.0  
 Atos Unify OpenScape First Response ESRP V9 before V9 R4.66.0  
 Atos Unify OpenScape First Response MSBF V2 before V2 R3.0.0  
 Atos Unify OpenScape Alarm Response Professional V4 and V5  
 Atos Unify OpenScape Xpert Clients V7 before V7 R4.2.0  
 Atos Unify OpenScape Xpert MLC V7 before V7 R4.2.0  
 Atos Unify OpenScape Xpert System Manager V7 before V7 R4.2.0  
 Atos Unify OpenScape Personal Edition V7 (Fixed in V7R 1.47.93 planned for 03.02.2023)  
 Atos Unify OpenScape Media Server V9 before 9.4.35.0 (delivered with OpenScape UC V10.3.17.0)  
 Atos Unify OpenScape 4000 Manager V8 and V10 before V10 R0.28.11 and V8 R2.22.17  
 Atos Unify OpenScape Accounting Management V4 (Fix planned until 28.02.23) and V5 before V5 R0.2.0  
 Atos Unify OpenScape Desk Phones CP SIP V1 before V1.9.5.0 and V2  
 Atos Unify OpenScape Desk Phones CP HFA V1 before V 1.6.4.2 and V2  
 Atos Unify OpenScape WLAN Phone WL4 before V3.1.6  
 AC Win SL V3  
 Atos Unify OpenScape Sesap V2 before V2 R1.1.5  
 Atos Unify OpenScape License Management CLC (Fix is planned until 28.04.23)  
 Atos Unify OpenScape Voice Trace Manager V8 before V8R0.9.8

*Products with affected License Management Interface (CLC)*

Atos Unify OpenScape Xpressions V7 R1.5.0 HF41 and higher  
 Atos Unify OpenScape Concierge V4

**Products confirmed not affected**

*Linux based applications using OpenSSL (follow instructions of the Linux operating system providers)*

Atos Unify OpenScape UC Application V10  
 Atos Unify OpenScape Common Management Platform V10  
 Atos Unify OpenScape Composer V2  
 Atos Unify OpenScape Voice Survival Authority

*Products that have been evaluated as not being affected*

Atos Unify OpenScape First Response PSS V1  
 Atos Unify OpenScape Extensions for MS Outlook V1 and V2  
 Atos Unify OpenScape Web Collaboration V7  
 Atos Unify OpenScape Fault Management V11 and V12  
 Atos Unify OpenScape DECT Phone S5 and SL5  
 Atos Unify OpenScape DECT Phone R6, S6 and SL6  
 Atos Unify OpenScape WLAN Phone WL3 (all versions) and WL4 V3.1.6 and higher

Atos Unify OpenScape WLAN Phone Wireless Service Gateway  
 HiPath CAP V3.0  
 HiPath DS-Win V4  
 Atos Unify OpenScape Backup & Recovery Services  
 Atos Unify OpenScape Business V3 R2 and higher  
 Atos Unify OpenScape Fusion for Office V2 R1.18.0 and higher  
 Atos Unify Virtual Care Collaboration Service V1 Sprint 90 and higher  
 Atos Unify OpenScape First GEMMA V3  
 Atos Unify OpenScape Deployment Service V10  
 Atos Unify OpenScape First Response ESAPP V1

**Additional Notes for the License Management:**

- The CLA (Customer License Agent) client interface that is exposed to CLS (Customer License Server) is not impacted
- The CLC (Customer License Client) interface to the CLA is impacted only if CLC and CLA run on separate machines. However where CLA runs on the same machine as the product software, then the CLC interface is not affected.
- The CLS interface is not impacted by the vulnerability

**Notes for Atos Unify OpenScape Enterprise Express V10** the evaluation of the following products apply:

If a product is affected, please follow the advisory for the respective product

Atos Unify OpenScape Voice (duplex deployments) V10  
 Atos Unify OpenScape Common Management Platform V10  
 Atos Unify OpenScape Deployment Service V10  
 Atos Unify OpenScape UC Application V10  
 Atos Unify OpenScape Media Server V9  
 Atos Unify OpenScape Concierge V4  
 Atos Unify OpenScape Contact Center V10  
 Atos Unify OpenScape Xpressions V7  
 Atos Unify OpenScape Voice Trace Manager V8

**Notes for Atos Unify OpenScape Voice (simplex deployments) V10**

Atos Unify OpenScape Voice (duplex deployments) V10  
 Atos Unify OpenScape Common Management Platform V10  
 Atos Unify OpenScape Deployment Service V10  
 Atos Unify OpenScape UC Application V10  
 Atos Unify OpenScape Media Server V9

## Recommended Actions

### Recommendations

- Products that are publicly exposing OpenSSL that are affected by CVE-2022-0778 should be patched as soon as there are patches available.
- Other products that are affected by CVE-2022-0778 should apply patches when available as part of regular patching of the product.
- Linux based applications using OpenSSL should be updated when patches are available

## References

### External References

- <https://www.openssl.org/news/secadv/20220315.txt>
- [BSI - CERT-Bund Meldungen - CB-K22/0321 Update 2](#)
- <https://github.com/drago-96/CVE-2022-0778>
- <https://www.suse.com/security/cve/CVE-2022-0778.html>
- [ubuntu.com/security/CVE-2022-0778](https://ubuntu.com/security/CVE-2022-0778)
- [security-tracker.debian.org/tracker/CVE-2022-0778](https://security-tracker.debian.org/tracker/CVE-2022-0778)
- [github.com/alpinelinux/docker-alpine/issues/243](https://github.com/alpinelinux/docker-alpine/issues/243)
- [blogs.gentoo.org/mgorny/2020/12/29/openssl-libressl-libretls-and-all-the-terminological-irony/](https://blogs.gentoo.org/mgorny/2020/12/29/openssl-libressl-libretls-and-all-the-terminological-irony/)

## Version Change History

Version	Date	Description
1.0	14.07.2022	- Initial release
1.1	18.07.2022	<ul style="list-style-type: none"> <li>- OpenScape Contact Center Application Server fixed in V10R4.5.0 and V11R0.4.0(available)</li> <li>- OpenScape Contact Center OpenMedia Connectors fixed in V1R0.5.0 (available)</li> <li>- OpenScape Contact Media Service fixed in V11R0.3.0 (available)</li> <li>- OpenScape Contact Center Server V10,V11 (fix planned in V10R4.7.0 for 16.09.2022 and V11R1.1.0 planned for 30.09.2022) (medium severity)</li> <li>- OpenScape Voice (Fix planned in V10R2.14.0 for 08/2022)</li> <li>- OpenScape 4000 Loadware fixed in V8R2.22.20 and V10R0.28.13 (available)</li> <li>- OpenScape Media Server fixed in 9.4.35.0 (delivered with OpenScape UC V10.3.17.0)</li> </ul>
1.2	04.08.2022	<ul style="list-style-type: none"> <li>- OpenScape Concierge V4 (License management interface affected (CLC))</li> <li>- OpenScape Voice (duplex deployments) V10 (Fix planned for 11/2022)</li> <li>- OpenScape Desk Phones CP SIP V1 and V2 (Fix planned for V1 R10)</li> <li>- OpenScape Desk Phones CP HFA V1 (Fix planned for V1 R6) and V2</li> <li>- OpenScape Desk Phones IP SIP V3 (reached end of support)</li> <li>- OpenScape Desk Phones IP HFA V3 (reached end of support)</li> <li>- OpenScape 4000 Platform (Fix planned in V8 R2.22.11 for 08/2022)</li> <li>- OpenScape 4000 V8 Assistant fixed in V8 R2.22.17 (available)</li> <li>- OpenScape 4000 V8 Manager fixed in V8 R2.22.17 (available)</li> <li>- OpenScape 4000 V10 CSTA fixed in V10 R0.28.9 (available)</li> </ul>

Version	Date	Description
1.3	12.09.2022	- OpenScape 4000 V8 Platform fixed in V8 R2.22.11 (available) - OpenScape 4000 V8 CSTA before fixed in V8 R2.22.13 (available)
1.4	08.11.2022	- OpenScape BCF fixed in V10. R0.0.0 - OpenScape Contact Cener V11 fixed in V11 R1.1.0 and V10 R8.4.0 - OpenScape Voice Trace Manager is fixed in V8R0.9.8
1.5	29.11.2022	- OpenScape First Response ESRP V9 fixed in V9 R4.66.0 - OpenScape Xpert Clients V7, MLC V7 and Systems Manager V7 fixed in V7 R4.2.0 - OpenScape Accounting Management V5 fixed in V5 R0.2.0 - OpenScape First Response MSBF fixed in verion V2R3..0..0
1.6	30.01.2023	- Atos Unify OpenScape Desk Phones CP HFA V1 fixed in version 1.6.4.2 - Atos Unify OpenScape Desk Phones CP SIP V1 fixed in V1.9.5.0 - Atos Unify OpenScape Accounting Management V4 (Fix planned until 28.02.23) - Atos Unify OpenScape License Management CLC (Fix is planned until 28.04.23) - Atos Unify OpenScape Personal Edition V7 (Fixed in V7R 1.47.93 planned for 03.02.2023)
1.7	31.01.2023	- Atos Unify OpenScape Voice V10 fixed in V10 R3.16.1
1.8	07.11.2023	- Atos Unify OpenScape Sesap V2 fixed in version V2 R1.1.5

Advisory: OBSO-2207-01, status: update release

Security Advisories are released as part of Mitel 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](mailto:obso@atos.net)

© Unify Software and Solutions GmbH & Co. KG 2023

Otto-Hahn-Ring 6

D-81739 München

[www.unify.com](http://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.