Security Advisory Report - OBSO-2207-01

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

Release Date:	2022-07-14 14:31:47
Last Update:	2022-08-04 09:55:12
Version:	1.2

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 indivdual 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 (planned in V10 R10.1.0 for 15.7.2022)
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 (Fix planned in V8 R2.22.11 for 08/2022)
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 (Fix planned in V8 R2.22.13 for 09/2022)
Atos Unify OpenScape Voice (duplex deployments) V10 (Fix planned for 11/2022)

Atos Unify 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)
Atos Unify OpenScape First Response ESRP V9
Atos Unify OpenScape First Response MSBF V2
Atos Unify OpenScape Alarm Response Professional V4 and V5
Atos Unify OpenScape Xpert Clients V7
Atos Unify OpenScape Xpert MLC V7
Atos Unify OpenScape Xpert System Manager V7
Atos Unify OpenScape Personal Edition V7
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 and V5
Atos Unify OpenScape Desk Phones CP SIP V1 and V2 (Fix planned for V1 R10)
Atos Unify OpenScape Desk Phones CP HFA V1 and V2 (Fix planned for V1 R6)
Atos Unify OpenScape WLAN Phone WL4 before V3.1.6
AC Win SL V3
Atos Unify OpenScape Sesap V2
Atos Unify OpenScape License Management CLC
Atos Unify OpenScape Voice Trace Manager V8

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
- security-tracker.debian.org/tracker/CVE-2022-0778
- github.com/alpinelinux/docker-alpine/issues/243
- 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	- OpenScape Contact Center Apllication Server fixed in V10R4.5.0 and V11R0.4.0(available) - OpenScape Contact Center OpenMedia Connectors fixed in V1R0.5.0 (available) - OpenScape Contact Media Service fixed in V11R0.3.0 (available) - 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) - OpenScape Voice (Fix planned in V10R2.14.0 for 08/2022) - OpenScape 4000 Loadware fixed in V8R2.22.20 and V10R0.28.13 (available) - OpenScape Media Server fixed in 9.4.35.0 (delivered with OpenScape UC V10.3.17.0)
1.2	04.08.2022	- OpenScape Concierge V4 (License management interface affected (CLC) - OpenScape Voice (duplex deployments) V10 (Fix planned for 11/2022) - OpenScape Desk Phones CP SIP V1 and V2 (Fix planned for V1 R10) - OpenScape Desk Phones CP HFA V1 and V2 (Fix planned for V1 R6) - OpenScape Desk Phones IP SIP V3 (reached end of support) - OpenScape Desk Phones IP HFA V3 (reached end of support) - OpenScape 4000 Platform (Fix planned in V8 R2.22.11 for 08/2022) - OpenScape 4000 V8 Assistant fixed in V8 R2.22.17 (available) - OpenScape 4000 V8 Manager fixed in V8 R2.22.17 (available) - OpenScape 4000 V10 CSTA fixed in V10 R0.28.9 (available)

Advisory: OBSO-2207-01, 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