

## Security Advisory Report - OBSO-2103-01

### OpenSSL Remote Denial of Service vulnerability (CVE-2021-3449)

Release Date: 2021-03-31 15:05:54

Last Update: 2021-04-21 11:56:24

#### Summary

OpenSSL contains a NULL pointer dereference vulnerability that may be exploited by an attacker to cause a denial of service condition on the affected system.

If a TLS client sends a specially crafted renegotiation ClientHello message, a remote attacker can crash the server process and cause a denial of service condition.

All OpenSSL 1.1.1 versions up to version 1.1.1j are affected by this issue. Users of these versions should upgrade to OpenSSL 1.1.1k. OpenSSL 1.0.2 is not impacted by this issue.

Atos Unify products that are using an affected OpenSSL version may be affected by this vulnerability. Evaluation of our products is ongoing.

The vulnerability is rated high with a CVSS 3.1 score of 7.5.

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

#### Details

An OpenSSL TLS server may crash if a TLS client sends a maliciously crafted renegotiation ClientHello message. If a TLSv1.2 renegotiation ClientHello omits the signature\_algorithms extension (where it was present in the initial ClientHello), but includes a signature\_algorithms\_cert extension then a NULL pointer dereference will result, leading to a crash and a denial of service attack.

A server is only vulnerable if it has TLSv1.2 and renegotiation enabled (which is the default configuration).

OpenSSL TLS clients are not impacted by this issue.

All OpenSSL 1.1.1 versions are affected by this issue. Users of these versions should upgrade to OpenSSL 1.1.1k.

OpenSSL 1.1.0 has not been evaluated but may be impacted by this issue as well.

OpenSSL 1.0.2 is not impacted by this issue.

Fixed in OpenSSL 1.1.1k (Affected 1.1.1-1.1.1j).

## Affected Products

### Affected products

OpenScape 4000 V10 Manager: (Fixed in V10 R0.28.6 / available)  
OpenScape 4000 V10 Assistant: (Fixed in V10 R0.28.6 / available)  
OpenScape 4000 V10 CSTA: (Fixed in V10 R0.28.3 / available)  
OpenScape 4000 V10 Platform: (Fixed in V10 R0.28.4 / available)  
OpenScape 4000 V10 Loadware: (Fixed in V10 R0.28.5 / available)  
OpenScape 4000 V8 from specific Loadware Hotfix V8 R2.22.10 (Fixed in V8 R2.22.14 / available) the SoftGate and STMIX loadware are affected  
OpenScape SBC V10 (Fixed in V10 R1.4.0 / available)  
OpenScape BCF V10 (Fixed in V10R9.3.0 / planned for 05/2021)  
OpenScape Branch V10 (Fixed in V10 R1.3.0 / available)  
OpenScape Xpert Client (Update to versions V7.3.0.1, V7.2.3 or newer / Fix planned in version V6.1.17 in 04/2021)  
OpenScape Contact Media Service V10 (Fix is planned / no plan date)  
OpenScape Business X Systems V3 (Fix is planned / no plan date)  
Circuit Meeting Room V1 (Fix is planned / no plan date)  
OpenScape Xpressions V7 (Fix planned for 05/2021)  
OpenScape Voice Trace Manager V8 (Fix planned for 05/2021)

### Products under investigation

OpenScape Accounting V4  
OpenScape Policy Store Service V1

### Applications running on Linux operating systems

Applications running on Suse, Debian and Ubuntu Linux operating systems may be affected (check references below)

OpenScape UC  
OpenScape Media Server  
OpenScape Xpert MLC  
OpenScape Common Management Portal  
OpenScape Composer  
OpenScape Business S Server

### Not Affected Products

OpenScape Voice V10 and V9  
OpenScape ESRP V9  
OpenScape 4000 V8 Manager  
OpenScape 4000 V8  
OpenScape 4000 V8 SoftGate and STMIX till specific Loadware Hotfix V8 R2.22.9  
OpenScape SBC V9  
OpenScape Branch V9  
Circuit Backend Services

Emergency Services Application V1

### **Not Affected Products (continued)**

OpenScape Fusion for IBM Notes V2  
OpenScape Fusion for Office V2  
Phones  
OpenScape Alarm Response

## **Recommended Actions**

### **Appliance based products**

Fixes will be provided for appliance based products that are affected. Implement the fixes that are provided.

### **Applications running on Linux operating systems**

Check whether you are using a vulnerable OpenSSL version and follow recommendations of Linux operation system providers.

Check advisories from Suse, Debian and Ubuntu(see references below)

Implement the fixes that are provided.

## **References**

<https://www.openssl.org/news/secadv/20210325.txt>  
[https://owasp.org/www-community/vulnerabilities/Null\\_Dereference](https://owasp.org/www-community/vulnerabilities/Null_Dereference)  
<https://www.suse.com/security/cve/CVE-2021-3449/>  
<https://security-tracker.debian.org/tracker/CVE-2021-3449>  
<https://ubuntu.com/security/notices/USN-4891-1>  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=2021-3449>  
<https://access.redhat.com/security/cve/cve-2021-3449>  
[https://bugzilla.redhat.com/show\\_bug.cgi?id=1941554](https://bugzilla.redhat.com/show_bug.cgi?id=1941554)  
<https://github.com/openssl/openssl/commit/02b1636fe3db274497304a3e95a4e32ced7e841b>  
<https://github.com/openssl/openssl/commit/2a40b7bc7b94dd7de897a74571e7024f0cf0d63b>  
<https://github.com/openssl/openssl/commit/39a140597d874e554b736885ac4dea16ac40a87a>  
<https://mta.openssl.org/pipermail/openssl-announce/2021-March/000196.html>  
<https://support2.windriver.com/index.php?page=security-notices&on=view&id=7055>  
<https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-openssl-2021-GHY28dJd>

<https://www.freebsd.org/security/advisories/FreeBSD-SA-21:07.openssl.asc>

---

Advisory: OBSO-2103-01, 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](mailto:obso@atos.net)

© Unify Software and Solutions GmbH & Co. KG 2021

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.