

# Security Advisory Report - OBSO-2101-01

## Amnesia:33 - Impact on Atos Unify Products

Release Date: 2021-01-08 16:22:05

Last Update: 2021-01-08 16:22:05

### Summary

Amnesia.33 relates to a set of vulnerabilities found in multiple open-source TCP/IP stacks. Atos Unify has evaluated its major product lines and the general impact on its products is medium to low.

The following affected components **are not used** within Atos Unify products:

- uIP-Contiki-OS (end-of-life [EOL]), Version 3.0 and prior
- uIP-Contiki-NG, Version 4.5 and prior
- uIP (EOL), Version 1.0 and prior
- picoTCP-NG, Version 1.7.0 and prior
- picoTCP (EOL), Version 1.7.0 and prior
- FNET, Version 4.6.3
- Nut/Net, Version 5.1 and prior

The following affected component may be delivered as part of the Linux operating system

- open-iscsi, Version 2.1.12 and prior

The major product lines have been evaluated. Refer to the **Affected Products** section for details on the evaluation.

### Details

The maintainer of open-iscsi has provided the following information and have rated severity to low:

<https://github.com/open-iscsi/open-iscsi/security/advisories/GHSA-r278-fm99-8rgp>

The Open-iSCSI developers have been made aware of multiple issues related to packet input processing in the uIP and related embedded TCP/IP networking stacks. The iscsiui tool in the Open-iSCSI project contains a forked copy of the uIP code.

After consideration of the disclosed vulnerabilities, only three were found to have matching code in the iscsiui source: CVE-2020-17437, CVE-2020-13988 and CVE-2020-13987. Given that iscsiui uses the uIP stack only for DHCP operations on specific offloading iSCSI hardware, it's believed that only **CVE-2020-13987** might have an exposed attack vector in the iscsiui process.

[CVE-2020-13987](#) (CVSS3.1: 7.5)

[CVE-2020-13988](#) (CVSS3.1: 7.5), deemed not be affecting iscsiui

[CVE-2020-17437](#) (CVSS3.1: 8.2), deemed not be affecting iscsiui

The iscsiui tool is only used for offloading iscsi in conjunction with a number of Broadcom/QLLogic network controllers.

For more information refer to:

<https://github.com/open-iscsi/open-iscsi/security/advisories/GHSA-r278-fm99-8rgp>

<https://fossies.org/linux/open-iscsi/iscsiui/README>

## Affected Products

**The following Appliance based products are not affected:**

OpenScape 4000  
OpenScape SBC / Branch / BCF  
OpenScape Xpert Clients  
OpenScape IP Cordless  
Circuit  
OpenScape Contact Media Service  
OpenScape Desk Phones  
OpenStage Phones  
Circuit Meeting Room  
OpenScape AlarmResponse  
OpenScape Business X (not affected in default configuration)

**The following Applications have been evaluated as not being affected in the default configuration**

OpenScape Xpert Multi Line Controller

All windows based applications are not affected.

**The following products may be affected under specific conditions**

OpenScape Voice / ESRP are not affected in the default configuration (A fix is planned)

**The following product are not directly affected, however the operating system may be affected under specific conditions**

OpenScape Business S  
OpenScape UC Application  
OpenScape Common Management Portal

## Recommended Actions

Check whether you are affected:

- Check whether iscsi is used at all
- If iscsi is used check whether iscsiuiio is running on your system used in conjunction with a relevant Broadcom/QLLogic network controller

If the system is affected:

- Check Suse Security Advisories for updates (see references below)
- Update openiscsi package to version 2.1.3 (when updates are available)

## References

General Information

- [AMNESIA:33 | RESEARCH REPORT](#)
- [ICS Advisory \(ICSA-20-343-01\)](#)
- [https://www.bsi.bund.de/SharedDocs/Warnmeldungen/DE/CB/2020/12/warnmeldung\\_cb-k20-1208.html](https://www.bsi.bund.de/SharedDocs/Warnmeldungen/DE/CB/2020/12/warnmeldung_cb-k20-1208.html)

openiscsi related information

- <https://github.com/open-iscsi/open-iscsi/security/advisories/GHSA-r278-fm99-8rgp>
- <https://fossies.org/linux/open-iscsi/iscsiuiio/README>

Suse Security Advisories

- <https://www.suse.com/security/cve/CVE-2020-13987/>
- <https://www.suse.com/security/cve/CVE-2020-13988/>
- <https://www.suse.com/security/cve/CVE-2020-17437/>
- <https://www.suse.com/security/cve/CVE-2020-17438/>

---

Advisory: OBSO-2101-01, 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](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.