Security Advisory Report - OBSO-2101-01

Amnesia:33 - Impact on Atos Unify Products

Release Date:	2021-01-08 16:22:05
Last Update:	2022-09-01 14:54:09
Version:	1.1

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 iscsiuio 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 iscsiuio source: CVE-2020-17437, CVE-2020-13988 and CVE-2020-13987. Given that iscsiuio 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 iscsiuio process.

CVE-2020-13987 (CVSS3.1: 7.5)
CVE-2020-13988 (CVSS3.1: 7.5), deemed not be affecting iscsiuio

CVE-2020-17437 (CVSS3.1: 8.2), deemed not be affecting iscsiuio

The iscsiuio tool is only used for offloading iscsi in conjunction with a number of Broadcom/QLogic 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/iscsiuio/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 (the following fixes have been provided)
open-iscsi package has been removed in the following versions:
OpenScape Voice versions V10R1.8.0, V9R4.48.12, V9R3.34.26 and higher
OpenScape ESRP V9R4.62.0 and higher

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 iscsiuio is running on your system used in conjunction with a relevant Broadcom/QLogic 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

openiscsi related information

- https://github.com/open-iscsi/open-iscsi/security/advisories/GHSA-r278-fm99-8rgp
- https://fossies.org/linux/open-iscsi/iscsiuio/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/

Version Change History

Version	Date	Description
1.0	08.01.2021	- Initial release

Version	Date	Description
1.1	01.09.2022	- Added fix versions for OpenScape Voice and OpenScape ESRP

Advisory: OBSO-2101-01, 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