

Security Advisory Report - OBSO-1911-02

Sudo: Privilege escalation via potential bypass of Runas user restrictions (CVE-2019-14287)

Release Date: 2019-11-08 16:35:23

Last Update: 2019-11-19 18:51:23

Summary

Sudo, a program designed to provide limited super user privileges to specific users, when configured to allow a user to run commands as an arbitrary user via the ALL keyword in a Runas specification, allows to run commands as root by specifying the user ID -1 or 4294967295. This could allow a user with sufficient sudo privileges to run commands as root even if the Runas specification explicitly disallows root access.

Details

Details can be found in the sudo advisory at https://www.sudo.ws/alerts/minus_1_uid.html

Affected Products

Affected products:

None (so far)

Not affected products:

Product are either not using sudo or do not having a vulnerable sudo configuration

OpenScape Voice
OpenScape Business
OpenScape 4000
OpenScape SBC/Branch
Circuit
Circuit Meeting Room
OpenStage/OpenScape Desk Phone IP SIP/HFA
OpenScape Desk Phone CP SIP/HFA
OpenStage/OpenScape Deskphone TDM
OpenScape Xpert
OpenScape Alarm Response

Recommended Actions

For all other products that are delivered as applications on Linux operating systems:

This vulnerability affects all linux distributions that have sudo included into their distribution (Redhat, suse, ubuntu, debian).

- Check your sudo configuration for the reported vulnerability
- Update operating systems according to vendor/distributor advise

References

https://www.sudo.ws/alerts/minus_1_uid.html
<https://access.redhat.com/security/cve/cve-2019-14287>
<https://www.debian.org/security/2019/dsa-4543>
<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-14287>
<https://thehackernews.com/2019/10/linux-sudo-run-as-root-flaw.html>

Advisory: OBSO-1911-02, status: general release

Security Advisories are released as part of Unify's Vulnerability Intelligence Process. For more information see <https://www.unify.com/security/advisories>.

Contact and Disclaimer

OpenScape Baseline Security Office
obs@atos.net
© **Unify Software and Solutions GmbH & Co. KG** 2019
Otto-Hahn-Ring 6
D-81739 München
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.