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