Security Advisory Report - OBSO-2102-01

Sudo Buffer Overflow Vulnerability (CVE-2021-3156)

Release Date:	2021-02-04 14:41:33
Last Update:	2021-04-21 14:55:13

Summary

Sudo before 1.9.5p2 has a heap-based buffer overflow vulnerability, allowing privilege escalation to root via "sudoedit -s" and a command-line argument that ends with a single backslash character.
The exploitation of this vulnerability will allow an attacker that has access to an unprivileged account to elevate privileges to root.

The vulnerability is rated high.

Details

On 26th of January 2021 researchers from Qualys published a report regarding a heap-based buffer overflow vulnerability in Sudo. Sudo is a Unix program that enables users to execute commands as another user (with privileges of another user, including root) as specified by the security policy (default location of policy: /etc/sudoers). By exploiting this vulnerability, an unprivileged user which is able to execute commands on the system is able to use Sudo to gain root privileges on a vulnerable host.

The CVE-2021-3156 flaw affects all legacy versions from 1.8.2 to 1.8.31p2 and all stable versions from 1.9.0 to 1.9.5p1 in their default configuration.

The vulnerability is rated high with a CVSS score of 7.8.
CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H

Affected Products

Affected Products

Appliance based products

OpenScape Voice V10 and V9 (Fixed in V10R1.8.0 / available), for V9 use single load line update with V10 software release
OpenScape ESRP V9 (Fixed in V9R4.59.0 planned 04/21)
OpenScape SBC V10 and V9 (Fixed in V10R1.3.0 / available), for V9 use single load line update with V10 software release
OpenScape BCF V10 (Fixed in V10R9.3.0 / planned for 05/2021)
OpenScape Branch V10 and V9 (Fixed in V10R1.3.0 / available), for V9 use single load line update with V10 software release
OpenScape Xpert Clients V7, V6 and V5 (Fixed in versions V7.3.0.1, V7.2.3 / available, fix planned in

version V6.1.17 for 04/21)
Circuit Backend (Fixed)
OpenScape Policy Store Services (Fix planned / no plan date)

Applications using Linux operating systems

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

Not Affected Products

OpenScape 4000
OpenScape Business X Systems
OpenScape Contact Media Service
OpenScape UC Clients
Phones
OpenScape Alarm Response
OpenScape Emergency Services Application

All Windows based products are not affected.

Recommended Actions

Fixes will be provided for appliance based products

For applications using Linux operating systems:

- Check operating system suppliers for the availability of patches
  https://www.suse.com/security/cve/CVE-2021-3156.html
  https://security-tracker.debian.org/tracker/CVE-2021-3156
  https://ubuntu.com/security/cve-2021-3156
- Implement patches

References

https://www.qualys.com/2021/01/26/cve-2021-3156/baron-samedit-heap-based-overflow-sudo.txt
https://blog.qualys.com/vulnerabilities-research/2021/01/26/cve-2021-3156-heap-based-buffer-overflow-in-sudo-baron-samedit
https://www.sudo.ws/alerts/unescape_overflow.html
https://www.bleepingcomputer.com/news/security/new-linux-sudo-flaw-lets-local-users-gain-root-privileges/

http://cve.mitre.org/cgi-bin/cvename.cgi?name=2021-3156
https://www.suse.com/security/cve/CVE-2021-3156.html
https://security-tracker.debian.org/tracker/CVE-2021-3156
https://ubuntu.com/security/cve-2021-3156

Advisory: OBSO-2102-01, 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