CVE-2022-0031

MITRE | NVD | CVE.ORG | Print: PDF

Summary

CVE	CVE-2022-0031
State	PUBLIC
Assigner	psirt@paloaltonetworks.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2022-11-09 18:15:00 UTC
Updated	2022-11-10 15:57:00 UTC
Description	A local privilege escalation (PE) vulnerability in the Palo Alto Networks Cortex XSOAR engine software running on a Linux

Risk And Classification

Problem Types: CWE-345

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Linux	Linux Kernel	-	All	All	All
Application	Paloaltonetworks	Cortex Xsoar	6.5.0	2102531	All	All
Application	Paloaltonetworks	Cortex Xsoar	6.5.0	2410815	All	All
Application	Paloaltonetworks	Cortex Xsoar	6.5.0	2583817	All	All
Application	Paloaltonetworks	Cortex Xsoar	6.6.0	2585049	All	All
Application	Paloaltonetworks	Cortex Xsoar	6.6.0	2889656	All	All
Application	Paloaltonetworks	Cortex Xsoar	6.6.0	3049220	All	All
Application	Paloaltonetworks	Cortex Xsoar	6.6.0	3124193	All	All
Application	Paloaltonetworks	Cortex Xsoar	6.8.0	3261002	All	All

References

Reference	Source	Link
CVE-2022-0031 Cortex XSOAR: Local Privilege Escalation (PE) Vulnerability in Cortex XSOAR Engine	MISC	security.paloaltonetwo
CVE Program record	CVE.ORG	www.cve.org
NVD vulnerability detail	NVD	nvd.nist.gov

No vendor comments have been submitted for this CVE.

There are currently no legacy QID mappings associated with this CVE.

CVE.report and Source URL Uptime Status status.cve.report