CVE-2021-3044

MITRE | NVD | CVE.ORG | Print: PDF

Summary

CVE	CVE-2021-3044
State	PUBLIC
Assigner	psirt@paloaltonetworks.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2021-06-22 18:15:00 UTC
Updated	2022-07-14 15:58:00 UTC
Description	An improper authorization vulnerability in Palo Alto Networks Cortex XSOAR enables a remote unauthenticated attacker wi

Risk And Classification

Problem Types: NVD-CWE-Other

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Paloaltonetworks	Cortex Xsoar	6.1.0	1016923	All	All
Application	Paloaltonetworks	Cortex Xsoar	6.2.0	-	All	All

References

Reference	Source	Link	Tags
CVE-2021-3044 Cortex XSOAR: Unauthorized Usage of the REST API	MISC	security.paloaltonetworks.com	
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical, analysis

Vendor Comments And Credit

Discovery Credit

LEGACY: This issue was found during internal security review.

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

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