CVE-2022-0020

MITRE | NVD | CVE.ORG | Print: PDF

Summary

CVE	CVE-2022-0020
State	PUBLIC
Assigner	psirt@paloaltonetworks.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2022-02-10 18:15:00 UTC
Updated	2023-04-10 20:15:00 UTC
Description	A stored cross-site scripting (XSS) vulnerability in Palo Alto Network Cortex XSOAR web interface enables an authenticated

Risk And Classification

Problem Types: CWE-79

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Paloaltonetworks	Cortex Xsoar	6.1.0	-	All	All
Application	Paloaltonetworks	Cortex Xsoar	6.1.0	1016923	All	All
Application	Paloaltonetworks	Cortex Xsoar	6.1.0	1031903	All	All
Application	Paloaltonetworks	Cortex Xsoar	6.1.0	1077664	All	All
Application	Paloaltonetworks	Cortex Xsoar	6.1.0	1209934	All	All
Application	Paloaltonetworks	Cortex Xsoar	6.1.0	1271079	All	All
Application	Paloaltonetworks	Cortex Xsoar	6.1.0	848144	All	All
Application	Paloaltonetworks	Cortex Xsoar	6.2.0	-	All	All
Application	Paloaltonetworks	Cortex Xsoar	6.2.0	1271082	All	All
Application	Paloaltonetworks	Cortex Xsoar	6.2.0	1321594	All	All
Application	Paloaltonetworks	Cortex Xsoar	6.2.0	1473927	All	All
Application	Paloaltonetworks	Cortex Xsoar	6.2.0	1578666	All	All
Application	Paloaltonetworks	Cortex Xsoar	6.2.0	1822745	All	All

References

Reference	Source	Link
Palo Alto Cortex XSOAR 6.5.0 Cross Site Scripting ≈ Packet Storm	MISC	packetstormsecurity.com

CVE-2022-0020 Cortex XSOAR: Stored Cross-Site Scripting (XSS) Vulnerability in Web Interface	CONFIRM	security.paloaltonetworks.cor
CVE Program record	CVE.ORG	www.cve.org
NVD vulnerability detail	NVD	nvd.nist.gov

Vendor Comments And Credit

Discovery Credit

LEGACY: Palo Alto Networks thanks Ömür Uğur of Türk Telekom for discovering and reporting this issue.

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