CVE-2021-3051

MITRE | NVD | CVE.ORG | Print: PDF

Summary

CVE	CVE-2021-3051
State	PUBLIC
Assigner	psirt@paloaltonetworks.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2021-09-08 17:15:00 UTC
Updated	2021-09-17 14:47:00 UTC
Description	An improper verification of cryptographic signature vulnerability exists in Cortex XSOAR SAML authentication that enables a

Risk And Classification

Problem Types: CWE-347

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Paloaltonetworks	Cortex Xsoar	5.5.0	-	All	All
Application	Paloaltonetworks	Cortex Xsoar	5.5.0	70066	All	All
Application	Paloaltonetworks	Cortex Xsoar	5.5.0	73387	All	All
Application	Paloaltonetworks	Cortex Xsoar	5.5.0	75211	All	All
Application	Paloaltonetworks	Cortex Xsoar	5.5.0	78518	All	All
Application	Paloaltonetworks	Cortex Xsoar	5.5.0	94592	All	All
Application	Paloaltonetworks	Cortex Xsoar	6.0.2	-	All	All
Application	Paloaltonetworks	Cortex Xsoar	6.0.2	90947	All	All
Application	Paloaltonetworks	Cortex Xsoar	6.0.2	93351	All	All
Application	Paloaltonetworks	Cortex Xsoar	6.0.2	94597	All	All
Application	Paloaltonetworks	Cortex Xsoar	6.0.2	97682	All	All
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

References

Reference	Source	Link	Tags
CVE-2021-3051 Cortex XSOAR: Authentication Bypass in SAML Authentication	CONFIRM	security.paloaltonetworks.com	
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical, an

Vendor Comments And Credit

Discovery Credit

LEGACY: This issue was found by a customer of Palo Alto Networks during a security review.

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