



CVE-2021-3034

[MITRE](#)[NVD](#)[CVE.ORG](#)[Print: PDF](#)

Summary

CVE	CVE-2021-3034
State	PUBLIC
Assigner	psirt@paloaltonetworks.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2021-03-10 18:15:00 UTC
Updated	2021-03-24 01:56:00 UTC
Description	An information exposure through log file vulnerability exists in Cortex XSOAR software where the secrets configured for the

Risk And Classification

Problem Types: CWE-532

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Paloaltonetworks	Cortex Xsoar	5.5.0	All	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	6.0.1	All	All	All
Application	Paloaltonetworks	Cortex Xsoar	6.0.1	81077	All	All
Application	Paloaltonetworks	Cortex Xsoar	6.0.2	All	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	All

References

Reference	Source	Link
-----------	--------	------

CVE-2021-3034 Cortex XSOAR: Secrets for SAML single sign-on (SSO) integration may be logged in system logs	CONFIRM	security.palo
CVE Program record	CVE.ORG	www.cve.or
NVD vulnerability detail	NVD	nvd.nist.gov

Vendor Comments And Credit

Discovery Credit

LEGACY: Palo Alto Networks thanks Martin Spielmann and Stefan Lubienetzki for discovering and reporting this issue.

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

© [CVE.report](#) 2026 |

Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, completeness or usefulness of any information, opinion, advice or other content. EACH USER WILL BE SOLELY RESPONSIBLE FOR ANY consequences of his or her direct or indirect use of this web site. ALL WARRANTIES OF ANY KIND ARE EXPRESSLY DISCLAIMED. This site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE, CWE, and OVAL are registered trademarks of [The MITRE Corporation](#) and the authoritative source of CVE content is [MITRE's CVE web site](#). This site includes MITRE data granted under the following [license](#).

CVE.report and Source URL Uptime Status [status.cve.report](#)