



CVE-2022-0014

[MITRE](#)[NVD](#)[CVE.ORG](#)[Print: PDF !\[\]\(e3f8612927870f2e0f9f5989e6dd3064_img.jpg\)](#)

Summary

CVE	CVE-2022-0014
State	PUBLIC
Assigner	psirt@paloaltonetworks.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2022-01-12 18:15:00 UTC
Updated	2022-01-19 19:21:00 UTC
Description	An untrusted search path vulnerability exists in the Palo Alto Networks Cortex XDR agent that enables a local attacker with

Risk And Classification

Problem Types: CWE-426

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Microsoft	Windows	-	All	All	All
Application	Paloaltonetworks	Cortex Xdr Agent	All	All	All	All

References

Reference	Source	Link
CVE-2022-0014 Cortex XDR Agent: Unintended Program Execution When Using Live Terminal Session	MISC	security.paloaltonetworks.com
CVE Program record	CVE.ORG	www.cve.org
NVD vulnerability detail	NVD	nvd.nist.gov

Vendor Comments And Credit

Discovery Credit

LEGACY: This issue was found by Robert McCallum of Palo Alto Networks during an internal security review.

Legacy QID Mappings

[376472](#) Palo Alto Networks Cortex XDR Agent Multiple Vulnerabilities (CPATR-13408,CPATR-13480,CPATR-12633)

© [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](#)