



# CVE-2022-0015

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

## Summary

<b>CVE</b>	CVE-2022-0015
<b>State</b>	PUBLIC
<b>Assigner</b>	psirt@paloaltonetworks.com
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2022-01-12 18:15:00 UTC
<b>Updated</b>	2022-01-19 19:22:00 UTC
<b>Description</b>	A local privilege escalation (PE) vulnerability exists in the Palo Alto Networks Cortex XDR agent that enables an authenticat

## Risk And Classification

**Problem Types:** CWE-427

## NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Paloaltonetworks	Cortex Xdr Agent	All	All	All	All

## References

Reference	Source
CVE-2022-0015 Cortex XDR Agent: An Uncontrolled Search Path Element Leads to Local Privilege Escalation (PE) Vulnerability	MISC
CVE Program record	CVE.ORG
NVD vulnerability detail	NVD

## Vendor Comments And Credit

### Discovery Credit

**LEGACY:** Palo Alto Networks thanks Xavier DANEST of Decathlon for discovering and reporting this issue.

## Legacy QID Mappings

[376469](#) Palo Alto Networks Cortex XDR Agent Privilege Escalation (PE) Vulnerability (CPATR-13405, CPATR-9287)

© [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](#)**