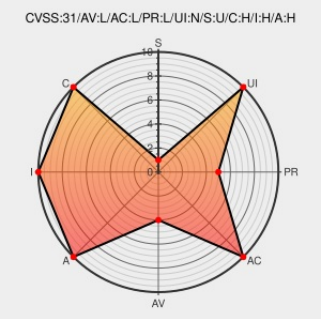
CVE-2020-2049

Published on: 12/09/2020 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:24:08 PM UTC

CVE-2020-2049

Source: Mitre | Source: NIST | CVE.ORG | Print: PDF



Certain versions of Windows from Microsoft contain the following vulnerability:

A local privilege escalation vulnerability exists in Palo Alto Networks Cortex XDR Agent on the Windows platform that allows an authenticated local Windows user to execute programs with SYSTEM privileges. This requires the user to have the privilege to create files in the Windows root directory. This issue impacts: All versions of Cortex XDR Agent 7.1 with content update 149 and earlier versions; All versions of Cortex XDR Agent 7.2 with content update 149 and earlier versions.

CVE-2020-2049 has been assigned by psirt@paloaltonetworks.com to track the vulnerability - currently rated as HIGH severity.

Vulnerability Patch/Work Around

This issue is mitigated by preventing local authenticated Windows users from creating files in the Windows root directory such as C:\.

CVSS3 Score: 7.8 - HIGH

Attack Vector	Attack Complexity	Privileges Required	User Interaction
LOCAL	LOW	LOW	NONE
Scope	**Confidentiality Impact**	**Integrity Impact**	**Availability Impact**
UNCHANGED	HIGH	HIGH	HIGH

CVSS2 Score: 7.2 - HIGH

Access Vector	Access Complexity	Authentication
LOCAL	LOW	NONE
Confidentiality Impact	**Integrity Impact**	**Availability Impact**
COMPLETE	COMPLETE	COMPLETE

CVE References

Description	Tags	Link
CVE-2020-2049 Cortex XDR Agent: Improper control of loaded DLL leads to local privilege escalation	Vendor Advisory security.paloaltonetworks.com text/html	MISC security.paloaltonetworks.com/CVE-2020-2049

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Microsoft	Windows	-	All	All	All
Operating System	Microsoft	Windows	-	All	All	All
Application	Paloaltonetworks	Cortex Xdr Agent	7.1	-	All	All
Application	Paloaltonetworks	Cortex Xdr Agent	7.1	content_update149	All	All
Application	Paloaltonetworks	Cortex Xdr Agent	7.2	-	All	All
Application	Paloaltonetworks	Cortex Xdr Agent	7.2	content_update149	All	All
Application	Paloaltonetworks	Cortex Xdr Agent	7.1	-	All	All
Application	Paloaltonetworks	Cortex Xdr Agent	7.1	content_update149	All	All
Application	Paloaltonetworks	Cortex Xdr Agent	7.2	-	All	All
Application	Paloaltonetworks	Cortex Xdr Agent	7.2	content_update149	All	All
Application	Paloaltonetworks	Cortex Xdr Agent	All	All	All	All
Application	Paloaltonetworks	Cortex Xdr Agent	All	All	All	All

cpe:2.3:o:microsoft:windows:-:*:*:*:*:*:*:*:

cpe:2.3:o:microsoft:windows:-:*:*:*:*:*:*:*:

cpe:2.3:a:paloaltonetworks:cortex_xdr_agent:7.1:-:*:*:*:*:*:*:

cpe:2.3:a:paloaltonetworks:cortex_xdr_agent:7.1:content_update149:*:*:*:*:*:*:

cpe:2.3:a:paloaltonetworks:cortex_xdr_agent:7.2:-:*:*:*:*:*:*:

cpe:2.3:a:paloaltonetworks:cortex_xdr_agent:7.2:content_update149:*:*:*:*:*:*:

cpe:2.3:a:paloaltonetworks:cortex_xdr_agent:7.1:-:*:*:*:*:*:*:

cpe:2.3:a:paloaltonetworks:cortex_xdr_agent:7.1:content_update149:*:*:*:*:*:*:

cpe:2.3:a:paloaltonetworks:cortex_xdr_agent:7.2:-:*:*:*:*:*:*:

cpe:2.3:a:paloaltonetworks:cortex_xdr_agent:7.2:content_update149:*:*:*:*:*:*:

cpe:2.3:a:paloaltonetworks:cortex_xdr_agent:*:*:*:*:*:*:*:*:

cpe:2.3:a:paloaltonetworks:cortex_xdr_agent:*:*:*:*:*:*:*:*:

Discovery Credit

Palo Alto Networks thanks Chris Au of PwC Hong Kong - Darklab and Xavier DANEST of Decathlon for discovering and reporting this issue.

← Previous ID

Next ID→