



# CVE-2022-0020

[MITRE](#)[NVD](#)[CVE.ORG](#)[Print: PDF !\[\]\(e3f8612927870f2e0f9f5989e6dd3064\_img.jpg\)](#)

## Summary

<b>CVE</b>	CVE-2022-0020
<b>State</b>	PUBLIC
<b>Assigner</b>	psirt@paloaltonetworks.com
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2022-02-10 18:15:00 UTC
<b>Updated</b>	2023-04-10 20:15:00 UTC
<b>Description</b>	A stored cross-site scripting (XSS) vulnerability in Palo Alto Network Cortex XSOAR web interface enables an authenticated

## Risk And Classification

**Problem Types:** CWE-79

## NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	<a href="#">Paloaltonetworks</a>	<a href="#">Cortex Xsoar</a>	6.1.0	-	All	All
Application	<a href="#">Paloaltonetworks</a>	<a href="#">Cortex Xsoar</a>	6.1.0	1016923	All	All
Application	<a href="#">Paloaltonetworks</a>	<a href="#">Cortex Xsoar</a>	6.1.0	1031903	All	All
Application	<a href="#">Paloaltonetworks</a>	<a href="#">Cortex Xsoar</a>	6.1.0	1077664	All	All
Application	<a href="#">Paloaltonetworks</a>	<a href="#">Cortex Xsoar</a>	6.1.0	1209934	All	All
Application	<a href="#">Paloaltonetworks</a>	<a href="#">Cortex Xsoar</a>	6.1.0	1271079	All	All
Application	<a href="#">Paloaltonetworks</a>	<a href="#">Cortex Xsoar</a>	6.1.0	848144	All	All
Application	<a href="#">Paloaltonetworks</a>	<a href="#">Cortex Xsoar</a>	6.2.0	-	All	All
Application	<a href="#">Paloaltonetworks</a>	<a href="#">Cortex Xsoar</a>	6.2.0	1271082	All	All
Application	<a href="#">Paloaltonetworks</a>	<a href="#">Cortex Xsoar</a>	6.2.0	1321594	All	All
Application	<a href="#">Paloaltonetworks</a>	<a href="#">Cortex Xsoar</a>	6.2.0	1473927	All	All
Application	<a href="#">Paloaltonetworks</a>	<a href="#">Cortex Xsoar</a>	6.2.0	1578666	All	All
Application	<a href="#">Paloaltonetworks</a>	<a href="#">Cortex Xsoar</a>	6.2.0	1822745	All	All

## References

Reference	Source	Link
Palo Alto Cortex XSOAR 6.5.0 Cross Site Scripting ≈ Packet Storm	MISC	<a href="https://packetstormsecurity.com">packetstormsecurity.com</a>

CVE-2022-0020 Cortex XSOAR: Stored Cross-Site Scripting (XSS) Vulnerability in Web Interface	CONFIRM	<a href="https://security.paloaltonetworks.com">security.paloaltonetworks.com</a>
CVE Program record	CVE.ORG	<a href="https://www.cve.org">www.cve.org</a>
NVD vulnerability detail	NVD	<a href="https://nvd.nist.gov">nvd.nist.gov</a>

## Vendor Comments And Credit

### Discovery Credit

**LEGACY:** Palo Alto Networks thanks Ömür Uğur of Türk Telekom for discovering and reporting this issue.

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

© [CVE.report](https://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](https://www.mitre.org) and the authoritative source of CVE content is [MITRE's CVE web site](https://www.mitre.org/cve). This site includes MITRE data granted under the following [license](https://www.mitre.org/licenses).

**CVE.report and Source URL Uptime Status** [status.cve.report](https://status.cve.report)