



# CVE-2022-20781

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

## Summary

<b>CVE</b>	CVE-2022-20781
<b>State</b>	PUBLIC
<b>Assigner</b>	psirt@cisco.com
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2022-04-06 19:15:00 UTC
<b>Updated</b>	2023-11-07 03:42:00 UTC
<b>Description</b>	A vulnerability in the web-based management interface of Cisco AsyncOS Software for Cisco Web Security Appliance (WS...

## Risk And Classification

**Problem Types:** CWE-79

## NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Cisco	Asyncos	All	All	All	All
Hardware	Cisco	Web Security Appliance	-	All	All	All

## References

Reference	Source	Link	Tags
20220406 Cisco Web Security Appliance Stored Cross-Site Scripting Vulnerability	CISCO	<a href="https://tools.cisco.com">tools.cisco.com</a>	
CVE Program record	CVE.ORG	<a href="https://www.cve.org">www.cve.org</a>	canonical
NVD vulnerability detail	NVD	<a href="https://nvd.nist.gov">nvd.nist.gov</a>	canonical, analysis

No vendor comments have been submitted for this CVE.

## Legacy QID Mappings

[317140](#) Cisco Web Security Appliance Stored Cross-Site Scripting Vulnerability (cisco-sa-wsa-stored-xss-XPsjghMY)

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](#)**