



# CVE-2023-20215

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

## Summary

<b>CVE</b>	CVE-2023-20215
<b>State</b>	PUBLIC
<b>Assigner</b>	psirt@cisco.com
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2023-08-03 22:15:00 UTC
<b>Updated</b>	2024-01-25 17:15:00 UTC
<b>Description</b>	A vulnerability in the scanning engines of Cisco AsyncOS Software for Cisco Secure Web Appliance could allow an unauth

## Risk And Classification

**Problem Types:** NVD-CWE-noinfo

## NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	<a href="#">Cisco</a>	<a href="#">Asyncos</a>	11.7.0-406	All	All	All
Operating System	<a href="#">Cisco</a>	<a href="#">Asyncos</a>	11.7.0-418	All	All	All
Operating System	<a href="#">Cisco</a>	<a href="#">Asyncos</a>	11.7.1-006	All	All	All
Operating System	<a href="#">Cisco</a>	<a href="#">Asyncos</a>	11.7.1-020	All	All	All
Operating System	<a href="#">Cisco</a>	<a href="#">Asyncos</a>	11.7.1-049	All	All	All
Operating System	<a href="#">Cisco</a>	<a href="#">Asyncos</a>	11.7.2-011	All	All	All
Operating System	<a href="#">Cisco</a>	<a href="#">Asyncos</a>	11.8.0-414	All	All	All
Operating System	<a href="#">Cisco</a>	<a href="#">Asyncos</a>	11.8.1-023	All	All	All
Operating System	<a href="#">Cisco</a>	<a href="#">Asyncos</a>	11.8.3-018	All	All	All
Operating System	<a href="#">Cisco</a>	<a href="#">Asyncos</a>	11.8.3-021	All	All	All
Operating System	<a href="#">Cisco</a>	<a href="#">Asyncos</a>	12.0.1-268	All	All	All
Operating System	<a href="#">Cisco</a>	<a href="#">Asyncos</a>	12.0.3-007	All	All	All
Operating System	<a href="#">Cisco</a>	<a href="#">Asyncos</a>	12.5.1-011	All	All	All
Operating System	<a href="#">Cisco</a>	<a href="#">Asyncos</a>	12.5.2-007	All	All	All
Operating System	<a href="#">Cisco</a>	<a href="#">Asyncos</a>	12.5.4-005	All	All	All
Operating System	<a href="#">Cisco</a>	<a href="#">Asyncos</a>	12.5.5-004	All	All	All
Operating System	<a href="#">Cisco</a>	<a href="#">Asyncos</a>	14.0.2-012	All	All	All

Operating System	Cisco	Asyncos	14.0.3-014	All	All	All
Operating System	Cisco	Asyncos	14.0.4-005	All	All	All
Operating System	Cisco	Asyncos	14.5.0-498	All	All	All
Operating System	Cisco	Asyncos	14.5.1-008	All	All	All
Operating System	Cisco	Asyncos	14.5.1-016	All	All	All
Hardware	Cisco	S195	-	All	All	All
Hardware	Cisco	S395	-	All	All	All
Hardware	Cisco	S695	-	All	All	All
Hardware	Cisco	Web Security Appliance S170	-	All	All	All
Hardware	Cisco	Web Security Appliance S190	-	All	All	All
Hardware	Cisco	Web Security Appliance S380	-	All	All	All
Hardware	Cisco	Web Security Appliance S390	-	All	All	All
Hardware	Cisco	Web Security Appliance S680	-	All	All	All
Hardware	Cisco	Web Security Appliance S690	-	All	All	All
Hardware	Cisco	Web Security Appliance S690x	-	All	All	All

## References

Reference	Source	Link	Tags
Cisco Secure Web Appliance Content Encoding Filter Bypass Vulnerability	MISC	<a href="https://sec.cloudapps.cisco.com">sec.cloudapps.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

[317338](#) Cisco Secure Web Appliance Content Encoding Filter Bypass Vulnerability (cisco-sa-wsa-bypass-vXvqwzsj)

© [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](https://status.cve.report)