



CVE-2021-1359

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

Summary

CVE	CVE-2021-1359
State	PUBLIC
Assigner	psirt@cisco.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2021-07-08 19:15:00 UTC
Updated	2023-11-07 03:28:00 UTC
Description	A vulnerability in the configuration management of Cisco AsyncOS for Cisco Web Security Appliance (WSA) could allow an

Risk And Classification

Problem Types: NVD-CWE-Other

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Cisco	Asyncos	All	All	All	All
Application	Cisco	Web Security Appliance	11.8.0-429	All	All	All
Application	Cisco	Web Security Appliance	11.8.0-453	All	All	All

References

Reference	Source	Link	Tags
Cisco Web Security Appliance Privilege Escalation Vulnerability	CISCO	tools.cisco.com	
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical, analysis

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

[316993](#) Cisco Web Security Appliance Privilege Escalation Vulnerability(cisco-sa-scr-web-priv-esc-k3HCGJZ)

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](#)