



CVE-2023-20057

[MITRE](#)[NVD](#)[CVE.ORG](#)[JSON API](#)[Print: PDF !\[\]\(003082e50e3009141f59bd5df831749f_img.jpg\)](#)

Summary

CVE	CVE-2023-20057
State	PUBLIC
Assigner	psirt@cisco.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2023-01-20 07:15:00 UTC
Updated	2024-01-25 17:15:00 UTC
Description	A vulnerability in the URL filtering mechanism of Cisco AsyncOS Software for Cisco Email Security Appliance (ESA) could e

Risk And Classification

Problem Types: CWE-74

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Cisco	Asyncos	-	All	All	All
Hardware	Cisco	Email Security Appliance C160	-	All	All	All
Hardware	Cisco	Email Security Appliance C170	-	All	All	All
Hardware	Cisco	Email Security Appliance C190	-	All	All	All
Hardware	Cisco	Email Security Appliance C370	-	All	All	All
Hardware	Cisco	Email Security Appliance C370d	-	All	All	All
Hardware	Cisco	Email Security Appliance C380	-	All	All	All
Hardware	Cisco	Email Security Appliance C390	-	All	All	All
Hardware	Cisco	Email Security Appliance C670	-	All	All	All
Hardware	Cisco	Email Security Appliance C680	-	All	All	All
Hardware	Cisco	Email Security Appliance C690	-	All	All	All
Hardware	Cisco	Email Security Appliance C690x	-	All	All	All
Hardware	Cisco	Email Security Appliance X1070	-	All	All	All

References

Reference	Source	Link	Tags
Cisco Email Security Appliance URL Filtering Bypass Vulnerability	MISC	sec.cloudapps.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			
317286 Cisco Email Security Appliance Uniform Resource Locator (URL) Filtering Bypass Vulnerability (cisco-sa-esa-url-bypass-WbMQqNJh)			

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

Free CVE JSON API cve.report/api

CVE.report and Source URL Uptime Status status.cve.report