



CVE-2021-1561

[MITRE](#)[NVD](#)[CVE.ORG](#)[Print: PDF !\[\]\(e3f8612927870f2e0f9f5989e6dd3064_img.jpg\)](#)

Summary

CVE	CVE-2021-1561
State	PUBLIC
Assigner	psirt@cisco.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2021-08-18 20:15:00 UTC
Updated	2023-11-07 03:28:00 UTC
Description	A vulnerability in the spam quarantine feature of Cisco Secure Email and Web Manager, formerly Cisco Security Management

Risk And Classification

Problem Types: CWE-287

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Hardware	Cisco	Secure Email And Web Manager	-	All	All	All
Operating System	Cisco	Secure Email And Web Manager	All	All	All	All

References

Reference	Source	Link	Tags
Cisco Secure Email and Web Manager Spam Quarantine Unauthorized Access Vulnerability	CISCO	tools.cisco.com	
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical, anal

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

317010 Cisco Secure Email and Web Manager Spam Quarantine Unauthorized Access Vulnerability(cisco-sa-sma-spam-jPxUXMk)

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](#)