

CVE-2025-20393

Cisco Multiple Products Improper Input Validation Vulnerability

CISA KEV since Dec 17, 2025

Actively exploited

A vulnerability in the Spam Quarantine feature of Cisco AsyncOS Software for Cisco Secure Email Gateway and Cisco Secure Email and Web Manager could allow an unauthenticated, remote attacker to execute arbitrary system commands on an affected device with root privileges. This vulnerability is due to insufficient validation of HTTP requests by the Spam Quarantine feature. An attacker could exploit this vulnerability by sending a crafted HTTP request to the affected device.

EVRs

75_{/100}

Urgent priority

CVSS V3.1

10.0

Critical · NVD

EPSS

0.324

98.3rd percentile · FIRST

CISA DEADLINE

Dec 24, 2025

CISA federal deadline · Overdue by 10 months

Signals behind the score

☒ counted in the score ☐ not counted

evidence for 6 of 8 signals

☒ CISA KEV	Listed in the catalog	☐ Vendor exploitation	Confirmed exploitation in the wild
☐ Ransomware	No known ransomware campaign association	☐ KEV recency	Added to CISA KEV within the last year
☒ EPSS	0.324 probability	☐ Pre-patch disclosure	Disclosure status unavailable
☒ CVSS	Base score 10.0	☐ Microsoft Exploitability Index	Not a Microsoft CVE

Remediation

Patch This Cycle Patch or fixed version identified

CISA required action: Apply mitigations per vendor instructions, follow applicable BOD 22-01 guidance for cloud services, or discontinue use of the product if mitigations are unavailable. **CISA note:** Please adhere to Cisco's guidelines to assess exposure and mitigate risks. Check for signs of potential compromise on all internet accessible Cisco products affected by this vulnerability. Apply any final mitigations provided by the vendor as soon as they become available.

Basis: CISA KEV required action

A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with root privileges.

Affected and fixed versions · 13 more affected products on the NVD record

PACKAGE	AFFECTED	FIXED IN	SOURCE
secure email gateway virtual appliance c100v	—	no fixed version listed	NVD
secure email gateway virtual appliance c300v	—	no fixed version listed	NVD
secure email gateway virtual appliance c600v	—	no fixed version listed	NVD
secure email and web manager virtual appliance m100v	—	no fixed version listed	NVD
secure email and web manager virtual appliance m300v	—	no fixed version listed	NVD

PACKAGE	AFFECTED	FIXED IN	SOURCE
secure email and web manager virtual appliance m600v	–	no fixed version listed	NVD
asyncos	$< 15.0.5-016$ $\geq 15.5 < 15.5.4-012$ $\geq 16.0 < 16.0.4-016$ $< 15.0.2-007$ $\geq 15.5 < 15.5.4-007$ $\geq 16.0 < 16.0.4-010$	15.0.5-016 · 15.5.4-012 · 16.0.4-016 · 15.0.2-007 · 15.5.4-007 · 16.0.4-010	NVD
secure email gateway c195	–	no fixed version listed	NVD

Sources

Vendor guidance github.com/advisories/GHSA-mrgj-cg36-fgq8

Additional guidance sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sma-attack-N9bf4

NVD nvd.nist.gov/vuln/detail/CVE-2025-20393

CISA KEV cisa.gov/known-exploited-vulnerabilities-catalog

ENISA EUVD euvd.enisa.europa.eu/vulnerability/EUVD-2025-203911

Current data evulnable.com/vulnerability-management/cve/CVE-2025-20393

Snapshot at generation time. EPSS can move quickly. A public exploit module is not evidence of active exploitation.