An Lárionad Náisiúnta Cibearshlándála
National Cyber Security Centre

NCSC #2512190211

NCSC Advisory

Cisco Secure Email Gateway, Cisco Secure Email and Web Manager

CVE-2025-20393

19th, January 2026

Update 1.1

STATUS: TLP:CLEAR

Recipients can spread this to the world, there is no limit on disclosure. Sources may use TLP:CLEAR when information carries minimal or no foreseeable risk of misuse, in accordance with applicable rules and procedures for public release. Subject to standard copyright rules, TLP:CLEAR information may be shared without restriction.

For more information on the Traffic Light Protocol, see https://www.first.org/tlp/. Please treat this document in accordance with the TLP assigned.

An Roinn Dlí agus Cirt,
Gnóthaí Baile agus Imirce
Department of Justice,
Home Affairs and Migration

Revision History

Revision	Date	Author	Description
1.0	19/12/25	NCSC	Initial Advisory
1.1	19/01/26	NCSC	Cisco Advisory Updates

Description

CVE ID: CVE-2025-20393

Published: 2025-12-17

Last Updated: 2026-01-19

Vendor: Cisco

Product: Cisco Secure Email Gateway and Cisco Secure Email and Web Manager

CVSS Score[1]: 10

Products Affected

This attack campaign targets Cisco Secure Email Gateway, both physical and virtual, and Cisco Secure Email and Web Manager appliances, both physical and virtual, when all the following conditions are met:

- The appliance is running a vulnerable release of Cisco AsyncOS Software.
- The appliance is configured with the Spam Quarantine feature.
- The Spam Quarantine feature is exposed to and reachable from the internet.

The Spam Quarantine feature is not enabled by default. Deployment guides for these products do not require this port to be directly exposed to the internet.

[1] https://www.first.org/cvss/

Product	Version
Cisco Secure Email	14.0.0-698
Cisco Secure Email	13.5.1-277
Cisco Secure Email	13.0.0-392
Cisco Secure Email	14.2.0-620
Cisco Secure Email	13.0.5-007
Cisco Secure Email	13.5.4-038
Cisco Secure Email	14.2.1-020
Cisco Secure Email	14.3.0-032
Cisco Secure Email	15.0.0-104
Cisco Secure Email	15.0.1-030
Cisco Secure Email	15.5.0-048
Cisco Secure Email	15.5.1-055
Cisco Secure Email	15.5.2-018
Cisco Secure Email	16.0.0-050
Cisco Secure Email	15.0.3-002
Cisco Secure Email	16.0.0-054
Cisco Secure Email	15.5.3-022
Cisco Secure Email	16.0.1-017
Cisco Secure Email and Web Manager	13.6.2-023
Cisco Secure Email and Web Manager	13.6.2-078
Cisco Secure Email and Web Manager	13.0.0-249
Cisco Secure Email and Web Manager	13.0.0-277
Cisco Secure Email and Web Manager	13.8.1-052
Cisco Secure Email and Web Manager	13.8.1-068
Cisco Secure Email and Web Manager	13.8.1-074
Cisco Secure Email and Web Manager	14.0.0-404
Cisco Secure Email and Web Manager	12.8.1-002
Cisco Secure Email and Web Manager	14.1.0-227

Cisco Secure Email and Web Manager	13.6.1-201
Cisco Secure Email and Web Manager	14.2.0-203
Cisco Secure Email and Web Manager	14.2.0-212
Cisco Secure Email and Web Manager	12.8.1-021
Cisco Secure Email and Web Manager	13.8.1-108
Cisco Secure Email and Web Manager	14.2.0-224
Cisco Secure Email and Web Manager	14.3.0-120
Cisco Secure Email and Web Manager	15.0.0-334
Cisco Secure Email and Web Manager	15.5.1-024
Cisco Secure Email and Web Manager	15.5.1-029
Cisco Secure Email and Web Manager	15.5.2-005
Cisco Secure Email and Web Manager	16.0.0-195
Cisco Secure Email and Web Manager	15.5.3-017
Cisco Secure Email and Web Manager	16.0.1-010
Cisco Secure Email and Web Manager	15.0.1-035
Cisco Secure Email and Web Manager	16.0.2-088

Impact

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

Common Weakness Enumeration (CWE)[2]: CWE-20: Improper Input Validation

Known Exploited Vulnerability (KEV) catalog[3]: Yes

Used by Ransomware Operators: N/A

Recommendations

The NCSC strongly recommends installing updates for vulnerable systems with the highest priority, after thorough testing. Affected organisations should review the latest release notes and install the relevant updates from Cisco.

- https://nvd.nist.gov/vuln/detail/CVE-2025-20393
- https://www.cve.org/CVERecord?id=CVE-2025-20393
- https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sma-attack-N9bf4
- https://www.cisa.gov/known-exploited-vulnerabilities-catalog?field_cve=CVE-2025-20393

[2] https://cwe.mitre.org

[3] https://www.cisa.gov/known-exploited-vulnerabilities-catalog