



An Láirionad Náisiúnta
Cibearshlándála
National Cyber
Security Centre

NCSC #2610150240

NCSC Advisory

Critical Zero-Day Vulnerability in Cisco Secure Email Gateway

CVE-2026-76519

15 October 2026

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.



Description

CVE ID: CVE-2026-76519**Published:** 2026-10-14**Vendor:** Cisco**Product:** Secure Email**CVSS Score¹:** 9.8

Products Affected

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

¹ <https://www.first.org/cvss/>





Cisco Secure Email	15.5.4-012
Cisco Secure Email	16.0.4-016
Cisco Secure Email	15.0.5-016
Cisco Secure Email	16.0.2-112
Cisco Secure Email	16.0.3-044

Impact

A vulnerability in the Advanced Malware Protection (AMP) feature of Cisco Secure Email Gateway could allow an unauthenticated, remote attacker to write arbitrary files on the underlying operating system.

This vulnerability is due to improper handling of email attachments when the file reputation service is enabled. An attacker could exploit this vulnerability by sending an email that contains a crafted attachment through an affected device. A successful exploit could allow the attacker to write arbitrary files and execute commands with root privileges on the underlying operating system.

Common Weakness Enumeration (CWE)²: CWE-23: Relative Path Traversal

Known Exploited Vulnerability (KEV) catalog³: Yes

Used by Ransomware Operators: N/A

² <https://cwe.mitre.org>

³ <https://www.cisa.gov/known-exploited-vulnerabilities-catalog>



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-2026-76519>
- <https://www.cve.org/CVERecord?id=CVE-2026-76519>
- <https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-esa-afw-zqYJkxp>
- https://www.cisa.gov/known-exploited-vulnerabilities-catalog?field_cve=CVE-2026-76519

