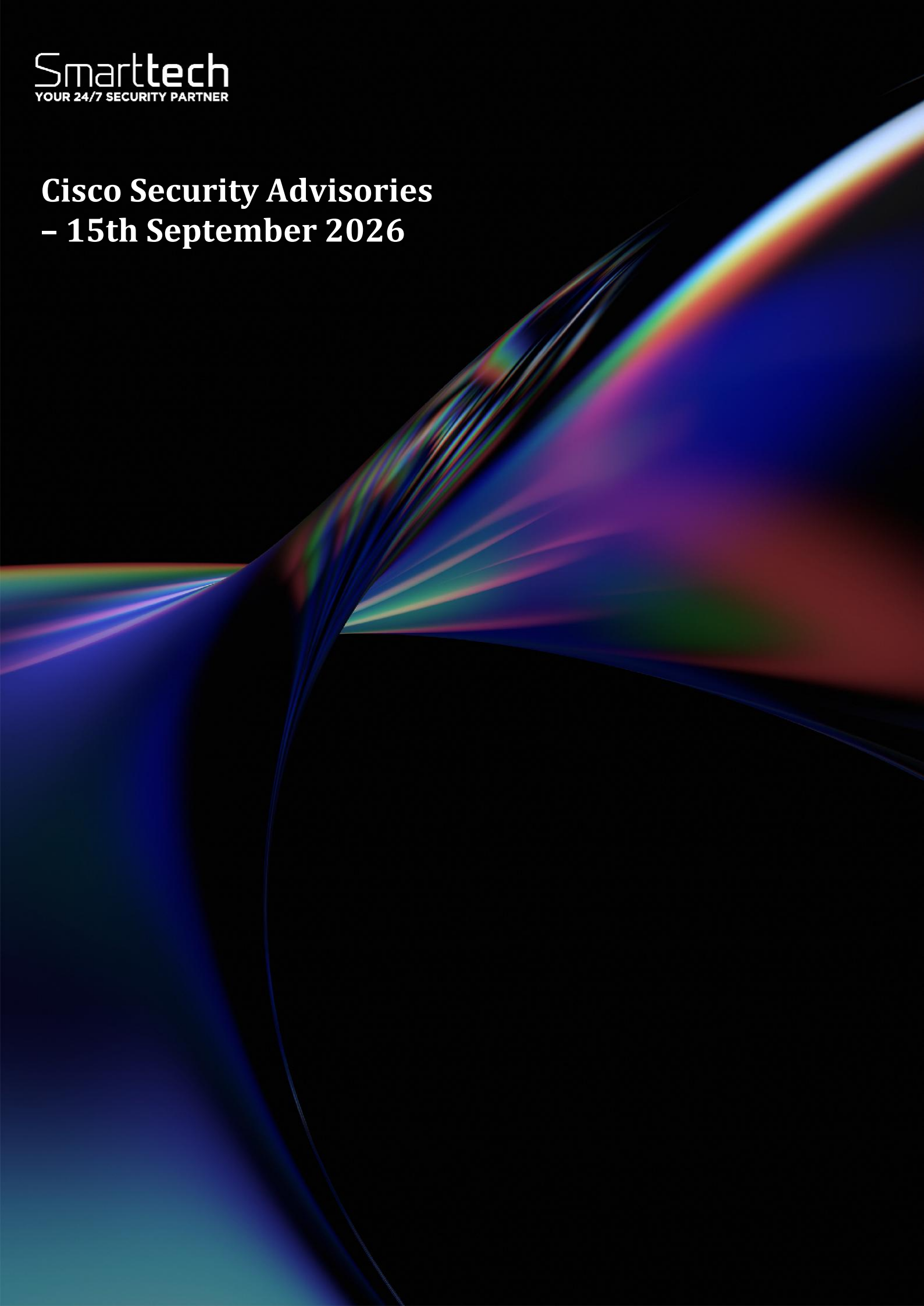
Smarttech
YOUR 24/7 SECURITY PARTNER

Cisco Security Advisories – 15th September 2026



Smarttech
YOUR 24/7 SECURITY PARTNER

Document ID	SMA-Threat Report
Document status	ISSUED
Issue Number	162
Authors	Dorin Constantin Banu < constantin.banu@smarttech247.com >
Verified by	Alin Curcan < alin.curcan@smarttech247.com >
Last modified	15th September 2026
Issue Date	14th September 2026

Threat Reports are reports created by Smarttech247 based on high and critical severity vulnerabilities that may have a high potential to be exploited in the wild i.e. vulnerabilities that are present in most used products by companies and do not have an auto-update option or they are usually not automatically updated in case that could lead to some service disruption. This report is usually created as soon as the vulnerability is released, therefore we strongly recommend that the information is reviewed, tests are performed and patches are applied before the first proof-of-concept is released.
Even though certain vulnerabilities may not have an active exploit in the wild at the time that we report on them, we take into consideration the wider risk and the impact it could have on systems, should an exploit like that be available after a while. Our duty is to report them on time and we recommend enterprises that, in order to keep critical business systems protected, they should consider, on average, ten working days to check whether or not the new vulnerability affects them, and if so, to implement actions in order to remove the risk.

Overview

Cisco disclosed multiple vulnerabilities affecting Cisco Secure Email Gateway and Cisco Secure Email and Web Manager, including a zero-day vulnerability (CVE-2026-76461) that is being actively exploited in the wild. These vulnerabilities could allow attackers to perform path traversal, bypass access controls, exploit improper resource lifecycle management, conduct command injections, SQL injection, code injection, and cross-site scripting (XSS) attacks, or trigger excessive resource consumption through improper input validation. Successful exploitation could result in arbitrary code execution with root privileges, information disclosure, unauthorized access, resource exhaustion, and service disruption.

Risk

Government:
- Large and medium government entities: **Critical**
- Small government entities: **Critical**

Businesses:
- Large and medium business entities: **Critical**
- Small business entities: **Critical**

Technical summary

Cisco Secure Email Gateway SQL Injection Vulnerability

CVE-2026-76461
CVSS Score: **9.8**

A vulnerability in the email parsing of Cisco AsyncOS Software for Cisco Secure Email Gateway could allow an unauthenticated, remote attacker to execute arbitrary commands with root privileges on the underlying operating system.

This vulnerability is due to insufficient validation in the email parsing logic. An attacker could exploit this vulnerability by sending a crafted email message that contains malicious SQL statements through an affected device. A successful exploit could allow the attacker to execute arbitrary SQL statements, leading to command execution with root privileges on the underlying operating system.

Indicators of Compromise (IoC)

To confirm any attempted exploitation of this vulnerability, review the mail_logs and look for suspicious SQL statements. If the device is part of a cluster, review the logs of each cluster device. The following is a non-exhaustive example of how a malicious SQL statement could be detected in the logs:

> cisco-esa> grep -i "COPY.*TO PROGRAM" [IronPort Text Mail Logs Log name - Default: mail_logs]

The presence of any entry in the output may indicate malicious activity.

On Cisco Secure Email Cloud, administrators without CLI access may not be able to independently check the described indicators of compromise. Cisco has directly contacted customers who own Cisco Secure Email Cloud devices on which malicious activity was detected.

Note: Upon successful exploitation of this vulnerability, threat actors may obtain command execution with root privileges. Because of this level of access, evidence of exploitation and indicators of compromise may be removed or hidden by the threat actors. Cisco strongly recommends that administrators cross-check the network logs and the firewall logs outside of the impacted device to identify any potential suspicious activity, including but not limited to unexpected uploads that were initiated from the affected device to external IP addresses or downloads from malicious IP addresses.

Affected Products

This vulnerability affects Cisco Secure Email Gateway, both physical and virtual, regardless of device configuration.

Fixed Releases

Cisco AsyncOS for Cisco Secure Email Gateway Software Release	First Fixed Release
15.5 and earlier	15.5.5-014*
16.0	16.0.4-302*
16.5	16.5.0-780

** Cisco strongly recommends that customers migrate to Release 16.5.0-780.*

Cisco Secure Email Gateway and Secure Email and Web Manager Security Hardening Release

As part of Cisco's ongoing commitment to proactive security and product quality, the Cisco Secure Email Gateway and Cisco Secure Email and Web Manager engineering team has conducted a comprehensive internal security review. This review resulted in software hardening releases that address multiple internally discovered vulnerabilities:

CVE-2026-76440
CVSS Score: **9.8**

Path traversal (covers improper limitation of a pathname to a restricted directory and improper link resolution before file access)

CVE-2026-76441
CVSS Score: **9.8**

Improper access control (covers authorization, authentication, privileges, and bypasses)

CVE-2026-20353
CVSS Score: **9.8**

Improper control of a resource through its lifetime (covers uncontrolled resource consumption, algorithmic complexity, recursion/iteration, deserialization, and improper resource initialization)

CVE-2026-76443
CVSS Score: **9.8**

Improper neutralization* (covers command, SQL, and code/eval injection, and cross-site scripting)
** One vulnerability that belongs to this vulnerability class is known to be actively exploited.*

CVE-2026-76442
CVSS Score: **7.5**

Improper validation of specified quantity in input (covers unbounded numeric fields that drive excessive resource consumption)

Affected Products

These vulnerabilities affect Cisco Secure Email Gateway and Cisco Secure Email and Web Manager, regardless of device configuration.

Fixed Releases

Cisco Secure Email Gateway Release	First Fixed Release
15.5 and earlier	15.5.5-014
16.0	Migrate to a fixed release.
16.5	16.5.0-780

Cisco Secure Email and Web Manager Release	First Fixed Release
15.5 and earlier	15.5.5-006
16.0	Migrate to a fixed release.
16.5	16.5.0-429

Recommendations

The **Smarttech247** team recommends the following actions**:**

- Apply the security updates provided by Cisco and upgrade all affected Cisco instances to a fixed software release as soon as operationally feasible. Cisco has indicated that no workarounds are available for these vulnerabilities.
- Implement the Principle of Least Privilege by limiting administrative access and regularly reviewing user accounts, roles, and permissions assigned within the SD-

WAN environment.

- Monitor system and authentication logs for signs of unauthorized privilege escalation attempts, suspicious administrative activity, or unexpected configuration changes, and forward logs to a centralized logging platform for analysis.
- Use vulnerability management and security monitoring solutions to identify affected systems, verify remediation status, and detect potential exploitation attempts.
- Ensure endpoint, network, and security monitoring solutions are up to date to provide visibility into malicious activity targeting SD-WAN infrastructure and management components.

References

https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-esa-inj-2bLVGmhX
https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-hardening-esa-dfCrfXkm
https://thehackernews.com/2026/09/cisco-secure-email-gateway-flaw.html

CVE

CVE-2026-76461
CVE-2026-76440
CVE-2026-76441
CVE-2026-20353
CVE-2026-76443
CVE-2026-76442

Smarttech
YOUR 24/7 SECURITY PARTNER

www.smarttech247.com