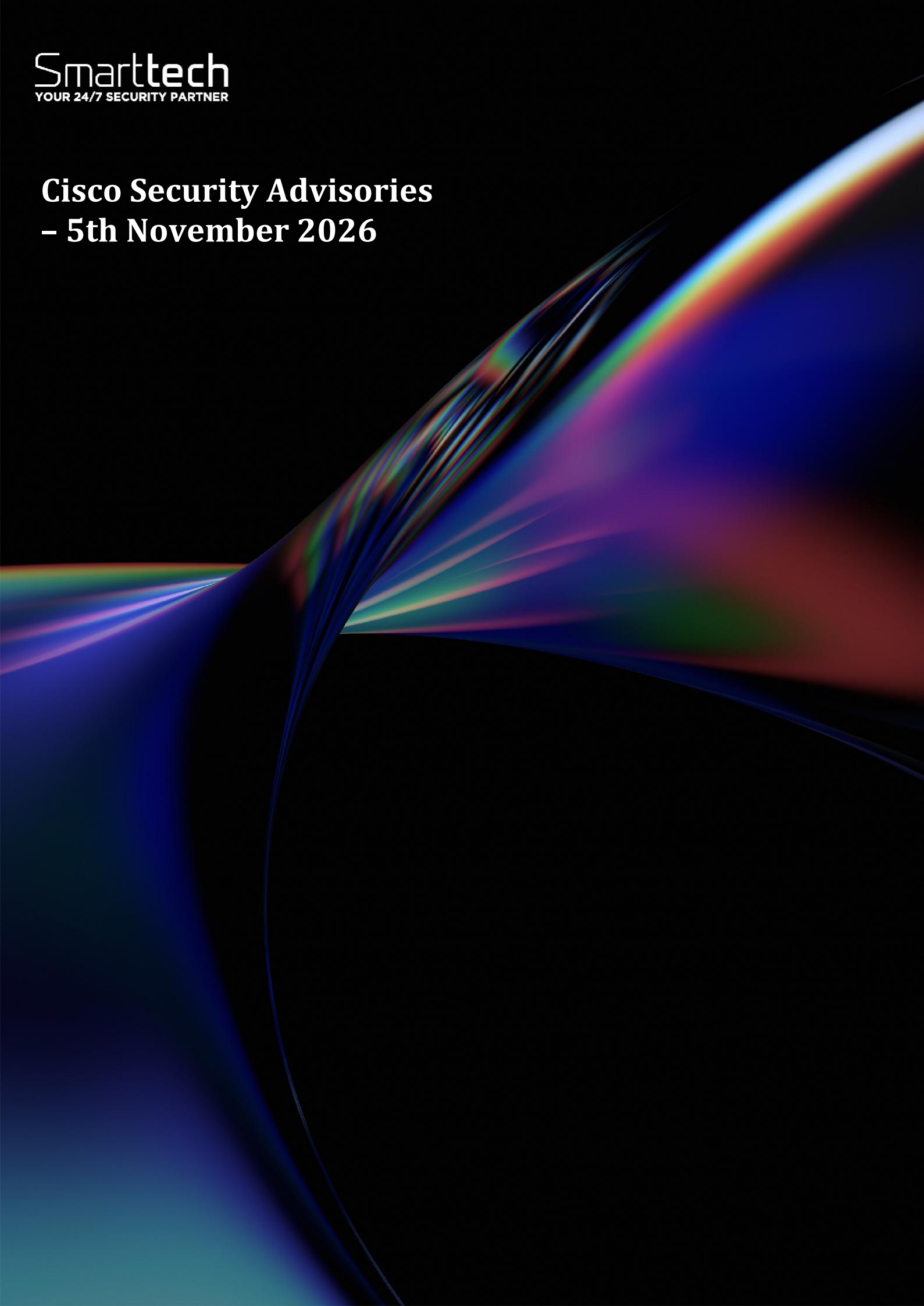
Smarttech
YOUR 24/7 SECURITY PARTNER

Cisco Security Advisories – 5th November 2026



Document ID	SMA-Threat Report
Document status	ISSUED
Issue Number	193
Authors	Dorin Constantin Banu < constantin.banu@smarttech247.com >
Verified by	Alin Curcan < alin.curcan@smarttech247.com >
Last modified	5th November 2026
Issue Date	4th November 2026

This document and any information therein are confidential property of Smarttech247 and without infringement neither the whole nor any extract may be disclosed, loaned, copied or used for manufacturing, provision of services or other purposes whatsoever without prior written consent of Smarttech247, and no liability is accepted for loss or damage from any cause whatsoever from the use of the document. Smarttech247 retain the right to alter the document at any time unless a written statement to the contrary has been appended.

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 has published security advisories addressing two vulnerabilities affecting Cisco products. Successful exploitation of these vulnerabilities could allow for cross-site scripting, remote code execution, or information disclosure.

Risk

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

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

Technical summary

Cisco Unified Communications Manager Cross-Site Scripting Vulnerability

CVE-2026-76419
CVSS Score: **6.1**

A vulnerability in the web-based management interface of Cisco Unified Communications Manager (Unified CM) and Cisco Unified Communications Manager Session Management Edition (Unified CM SME) could allow an unauthenticated, remote attacker to conduct a cross-site scripting (XSS) attack against a user of the interface.

This vulnerability exists because the web-based management interface does not properly validate user-supplied input. An attacker could exploit this vulnerability by persuading a user of the interface to click a crafted link. A successful exploit could allow the attacker to execute arbitrary script code in the context of the affected interface or access sensitive, browser-based information.

Affected Products

This vulnerability affected Cisco Unified CM and Cisco Unified CM SME, regardless of device configuration.

Fixed Releases

Cisco Unified CM and Unified CM SME Release	First Fixed Release
14	Migrate to a fixed release.
15	15SU5

Cisco UCS Central Software Remote Code Execution Vulnerability

CVE-2026-76506
CVSS Score: **7.6**

A vulnerability in the web-based management interface of Cisco UCS Central Software could allow an authenticated, remote attacker to achieve remote code execution or conduct information disclosure attacks on an affected device.

This vulnerability is due to insufficient validation of user-supplied input in an HTTP request. An attacker could exploit this vulnerability by sending a crafted HTTP request to an affected endpoint on an affected device. A successful exploit could allow the attacker to execute arbitrary commands, write arbitrary files to the filesystem, and obtain sensitive information. To exploit this vulnerability, the attacker must have valid user credentials on the affected device.

Affected Products

This vulnerability affects Cisco UCS Central Software, regardless of device configuration.

Fixed Releases

Cisco UCS Central Software	First Fixed Release
2.0 and earlier	Migrate to a fixed release.
2.1	2.1(2c)

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-cucm-xss-5mQn2U5z
https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-cucs-rce-LzHSFRDQ

CVE

CVE-2026-76419
CVE-2026-76506

Smarttech
YOUR 24/7 SECURITY PARTNER

www.smarttech247.com