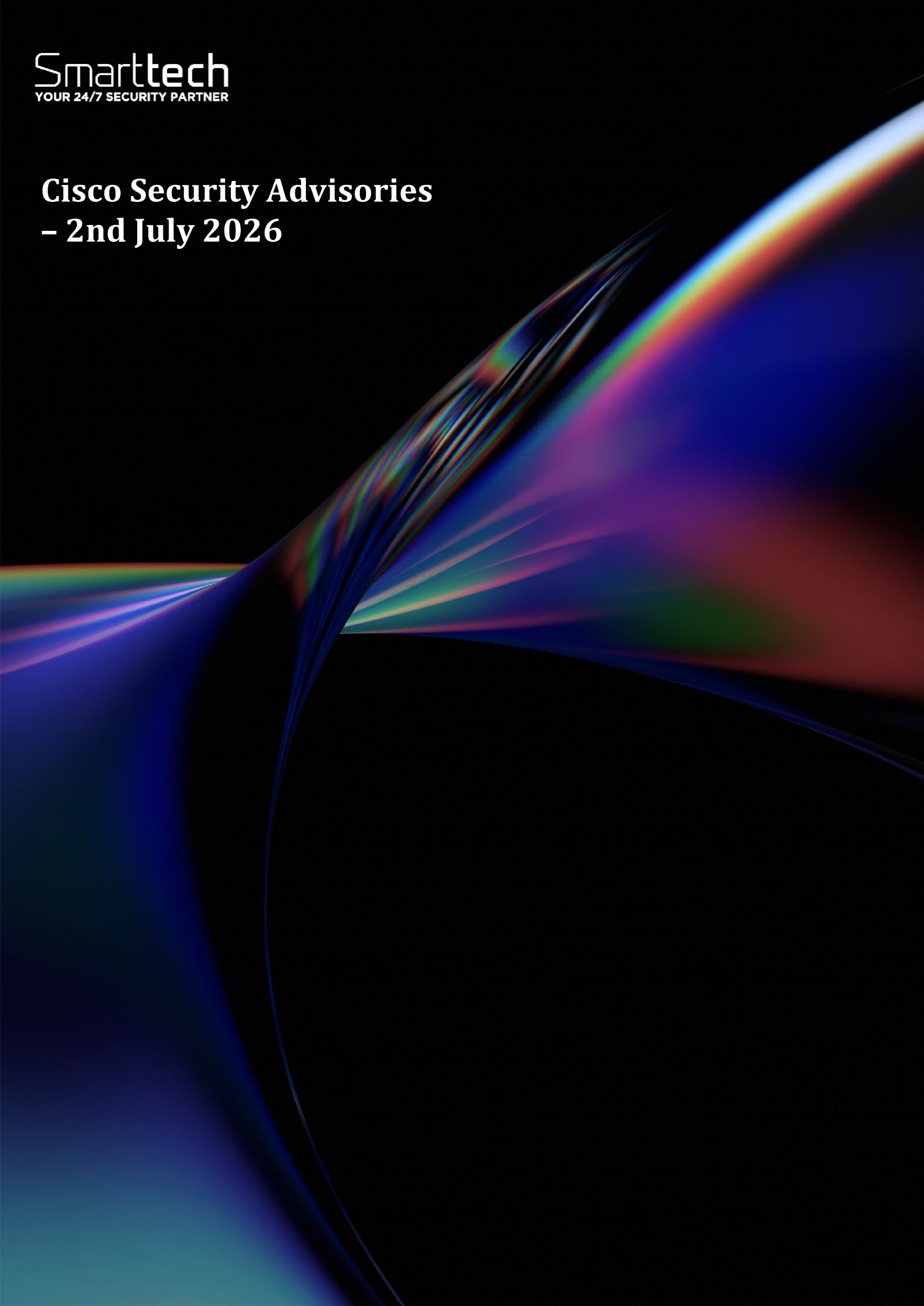
Smarttech
YOUR 24/7 SECURITY PARTNER

Cisco Security Advisories – 2nd July 2026



Document ID	SMA-Threat Report
Document status	ISSUED
Issue Number	109
Authors	Dorin Constantin Banu < constantin.banu@smarttech247.com >
Verified by	Alin Curcan < alin.curcan@smarttech247.com >
Last modified	2nd July 2026
Issue Date	1st July 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 Catalyst Center and the third-party component ClamAV integrated into Cisco products. These vulnerabilities could allow a remote attacker to disrupt affected systems or gain access to sensitive information. Successful exploitation could allow for information disclosure or cause a denial of service condition, impacting the availability of affected systems.

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 Catalyst Center Arbitrary File Read Vulnerability

CVE-2026-20191
CVSS Score: **7.5**

A vulnerability in Cisco Catalyst Center could allow an unauthenticated, remote attacker to read arbitrary files from a restricted container.

This vulnerability is due to insufficient validation of user-supplied input. An attacker could exploit this vulnerability by sending a crafted HTTP request to an affected device. A successful exploit could allow the attacker to read arbitrary files from a restricted container of the affected device.

ClamAV Vulnerabilities Affecting Cisco Products

CVE-2026-20216
CVSS Score: **7.5**

A vulnerability in the InstallShield file format parser of ClamAV could allow an unauthenticated, remote attacker to cause a DoS condition on an affected device.

This vulnerability is due to improper handling of temporary resources during file scanning. An attacker could exploit this vulnerability by submitting a crafted InstallShield file to be scanned by ClamAV on an affected device. A successful exploit could allow the attacker to terminate the ClamAV scanning process and temporarily consume available system resources, resulting in a DoS condition on the affected software.

CVE-2026-20213
CVSS Score: **7.5**

A vulnerability in the PE file format parser of ClamAV could allow an unauthenticated, remote attacker to cause a DoS condition, or possibly other expanded impacts, resulting from memory corruption on an affected device.

This vulnerability is due to improper boundary checks for content in PE files during scanning, which may result in an out-of-bounds buffer write. An attacker could exploit this vulnerability by submitting a crafted file that contains PE content to be scanned by ClamAV on an affected device. A successful exploit could allow the attacker to cause the ClamAV scanning process to terminate, resulting in a DoS condition on the affected software.

CVE-2026-20214
CVSS Score: **7.5**

A vulnerability in the FSG file format parser of ClamAV could allow an unauthenticated, remote attacker to cause a DoS condition, or possibly other expanded impacts, resulting from memory corruption on an affected device.

This vulnerability is due to improper boundary checks for content in FSG files during scanning, which may result in an out-of-bounds buffer write. An attacker could exploit this vulnerability by submitting a crafted file that contains portable executable content compressed with FSG to be scanned by ClamAV on an affected device. A successful exploit could allow the attacker to cause the ClamAV scanning process to terminate, resulting in a DoS condition on the affected software.

CVE-2026-20215
CVSS Score: **7.5**

A vulnerability in the 7z file format parser of ClamAV could allow an unauthenticated, remote attacker to cause a DoS condition, or possibly other expanded impacts, resulting from memory corruption on an affected device.

This vulnerability is due to improper boundary checks for content in 7z files during scanning, which may result in an out-of-bounds buffer write. An attacker could exploit this vulnerability by submitting a crafted file that contains 7z content to be scanned by ClamAV on an affected device. A successful exploit could allow the attacker to cause the ClamAV scanning process to terminate, resulting in a DoS condition on the affected software.

CVE-2026-20217
CVSS Score: **7.5**

A vulnerability in the PESpin file format parser of ClamAV could allow an unauthenticated, remote attacker to cause a DoS condition, or possibly other expanded impacts, resulting from memory corruption on an affected device.

This vulnerability is due to improper boundary checks for content in PESpin files during scanning, which may result in an out-of-bounds buffer write. An attacker could exploit this vulnerability by submitting a crafted file that contains PESpin content to be scanned by ClamAV on an affected device. A successful exploit could allow the attacker to cause the ClamAV scanning process to terminate, resulting in a DoS condition on the affected software.

CVE-2026-20243
CVSS Score: **7.5**

A vulnerability in the ALZ file format parser of ClamAV could allow an unauthenticated, remote attacker to cause a DoS condition, or possibly other expanded impacts, resulting from memory corruption on an affected device.

This vulnerability is due to improper boundary checks for content in ALZ files during scanning, which may result in an out-of-bounds buffer write. An attacker could exploit this vulnerability by submitting a crafted file that contains ALZ content to be scanned by ClamAV on an affected device. A successful exploit could allow the attacker to cause the ClamAV scanning process to terminate, resulting in a DoS condition on the affected software.

CVE-2026-20244
CVSS Score: **7.5**

A vulnerability in the DMG file format parser of ClamAV could allow an unauthenticated, remote attacker to cause a DoS condition, or possibly other expanded impacts, resulting from memory corruption on an affected device.

This vulnerability is due to improper boundary checks for content in DMG files during scanning, which may result in an integer overflow on 32-bit platforms only. An attacker could exploit this vulnerability by submitting a crafted file that contains DMG content to be scanned by ClamAV on an affected device. A successful exploit could allow the attacker to cause the ClamAV scanning process to terminate, resulting in a DoS condition on the affected software.

Affected Products

Cisco Catalyst Center Arbitrary File Read Vulnerability

This vulnerability affects Cisco Catalyst Center, both virtual and hardware appliances, regardless of device configuration.

Fixed Releases

Catalyst Center Hardware Appliances, Catalyst Center Virtual Appliances on AWS, and Catalyst Center Virtual Appliances on Azure

Cisco Catalyst Center Release	First Fixed Release
Earlier than 3.1	Not vulnerable
3.1	3.1.6 GSMU200

Catalyst Center Virtual Appliances on VMware ESXi

Cisco Catalyst Center Release	First Fixed Release
2.3.7	2.3.7.11-VA GSMU100
3.1	3.1.6 GSMU200

ClamAV Vulnerabilities Affecting Cisco Products

The following table lists Cisco products that are affected by the vulnerabilities that are described in this advisory. Customers should refer to the associated Cisco bug IDs for further details.

Fixed Releases

Affected Cisco Software Platform	Cisco Bug ID	First Fixed Release
Secure Endpoint Connector for Linux	CSCwt81503	1.29.0
Secure Endpoint Connector for Mac	CSCwt81504	1.27.2
Secure Endpoint Connector for Windows	CSCwt81501	8.6.2
Secure Endpoint Private Cloud	CSCwu55927	4.2.8 and later

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-catc-file-read-wLH2vf8X
https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-clamav-88cFYyxR

CVE

CVE-2026-20191
CVE-2026-20216
CVE-2026-20213
CVE-2026-20214
CVE-2026-20215
CVE-2026-20217
CVE-2026-20243
CVE-2026-20244

Smarttech
YOUR 24/7 SECURITY PARTNER

www.smarttech247.com