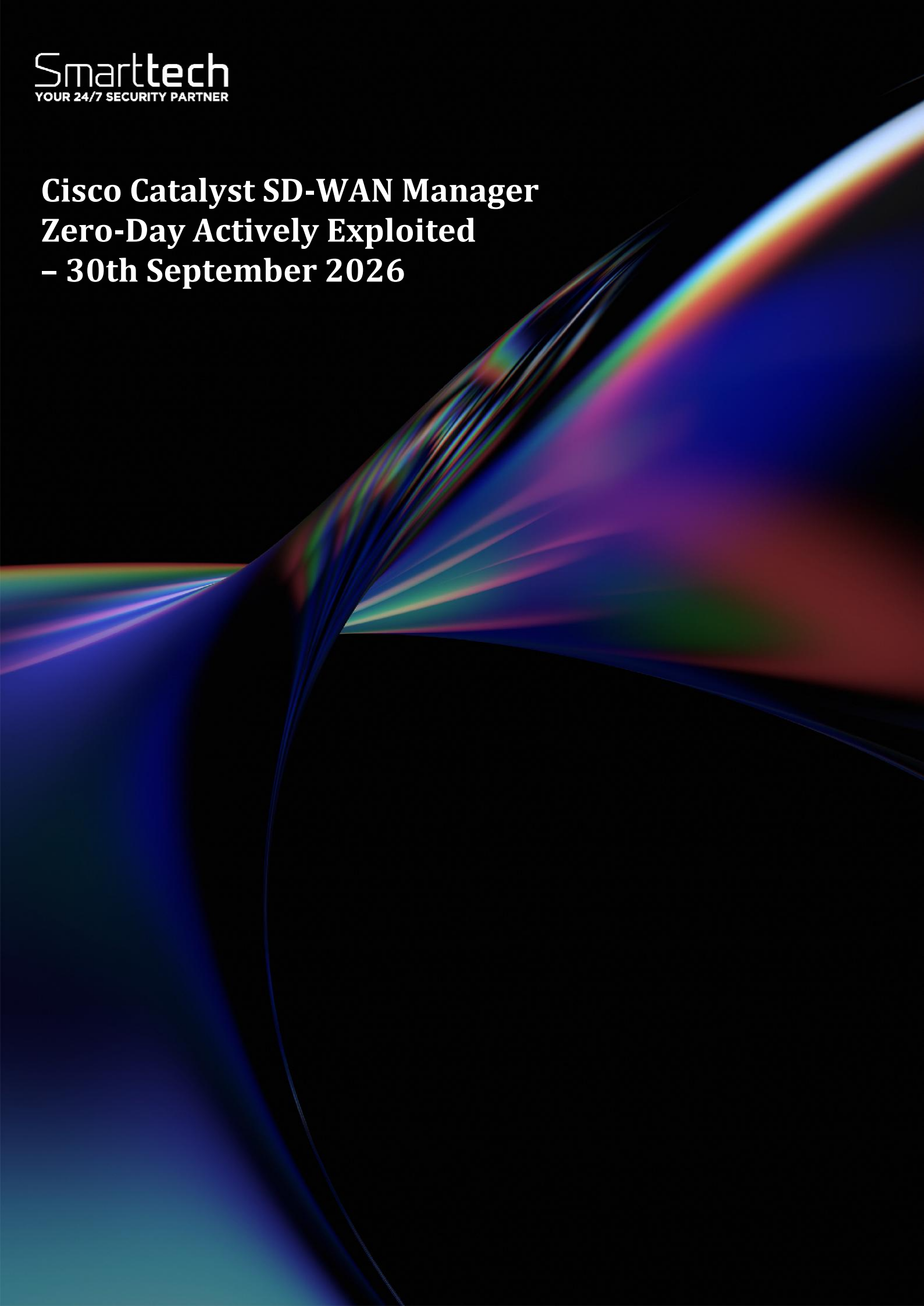


**Cisco Catalyst SD-WAN Manager
Zero-Day Actively Exploited
– 30th September 2026**



Document ID	SMA-Threat Report
Document status	ISSUED
Issue Number	172
Authors	Dorin Constantin Banu < constantin.banu@smarttech247.com >
Verified by	Alin Curcan < alin.curcan@smarttech247.com >
Last modified	30th September 2026
Issue Date	30th September 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 disclosed a critical zero-day vulnerability affecting Catalyst SD-WAN Manager that is being actively exploited in the wild. This vulnerability could allow attackers to bypass authentication controls through improper handling of URI encoding in HTTP requests. Successful exploitation could allow an attacker to gain access to the API as the admin user and obtain administrative control of the affected system.

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 Catalyst SD-WAN Manager API Authentication Bypass Vulnerability

CVE-2026-76504

CVSS Score: **9.8**

A vulnerability in the API session-based authentication management of Cisco Catalyst SD-WAN Manager could allow an unauthenticated, remote attacker to access an affected system with privileges of the admin user.

This vulnerability is due to improper handling of URI encoding in an HTTP request, which allows the request to bypass an authentication rule that is intended to restrict access to a specific API endpoint. An attacker could exploit this vulnerability by sending a crafted HTTP request to the API of the affected system. A successful exploit could allow the attacker to bypass authentication and gain access to the API as the admin user.

Indicators of Compromise (IoC)

Cisco Catalyst SD-WAN Manager systems that are exposed to the internet and that have ports exposed to the internet are at risk of exposure to compromise. In some instances, these indicators of compromise (IOCs) may occur during standard operations. Therefore, they must be assessed against normal network posture to identify and avoid false positives.

Important: These IOC examples show the use of %6a as the URI encoded character j in the request. This is only an example, and the vulnerability will allow any one character that is encoded in the request to be used to exploit this.

Customers are encouraged to audit the serviceproxy-access.log file, located at /var/log/nms/containers/service-proxy/serviceproxy-access.log, for entries that are related to j_security_check from unknown or unauthorized IP addresses, as shown in the following example:

```
[2026-09-29T23:11:13.948-05:00] "POST /%6a_security_check HTTP/1.1" 200 - 48
0 4 - "10.10.10.47,192.168.1.174" "Mozilla/5.0" "92980fc6-bb3c-4b67-8a6d-
af5ceb236d4c" "vmanage-9999.example.com" "127.0.0.1:8080"
```

Customers are encouraged to audit the vmanage-server.log file, located at /var/log/nms/vmanage-server.log, for entries that are related to j_security_check from unknown or unauthorized IP addresses, specifically being called for users that include names starting with viptela-reserved-, as shown in the following example:

```
29-Sep-2026 23:11:13,952 CDT [] [vManage-new] [UserUtils] (default task-127462)
|default| Request Stored in Map is (/%6a_security_check) for user (viptela-reserved-
..)
```

For help determining if Cisco Catalyst SD-WAN Manager has been compromised, customers may open a case with the Cisco Technical Assistance Center (TAC). Cisco TAC cases should be opened as a Severity 3 with the CVE-ID CVE-2026-76504 in the title. Before opening a new TAC case, customers are encouraged to use the request admin-tech command from the Cisco Catalyst SD-WAN Manager (vManage) in the SD-WAN deployment so that the admin-tech file can be provided to the Cisco TAC for review.

The viptela-reserved system service accounts are documented in the [Authentication, Authorization, and Accounting](#) section of the Cisco Catalyst SD-WAN Systems and Interfaces Configuration Guide.

Affected Products

This vulnerability affects Cisco Catalyst SD-WAN Manager, regardless of system configuration.

Fixed Releases

Cisco Catalyst SD-WAN Software Release	First Fixed Release
Earlier than 20.9	Migrate to a fixed release.
20.9	20.9.10.1
20.12	20.12.8.2
20.15	20.15.6.1

20.18	20.18.4.1
26.1	26.1.2.1
26.2	26.2.1

Note: Cisco has also addressed this vulnerability in Cisco SD-WAN Cloud (Cisco Managed) Release 20.15.605, which is cloud based. No user action is required. Customers can determine the current remediation status or software version by using the Help function in the service GUI.

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-sdwan-webauth-xr8beuuU>

CVE

CVE-2026-76504

