
Cisco Zero-Day Exploited

SD-WAN Controller Maximum Severity Flaw

Cisco Zero-Day Exploited: SD-WAN Controller Maximum Severity Flaw

A sophisticated threat actor is actively exploiting a maximum-severity vulnerability in Cisco's Catalyst SD-WAN infrastructure, giving them unauthorized administrative access to network controllers. The max severity flaw allows remote attackers to bypass authentication entirely and log in as a high-privileged internal user. Once inside, attackers can manipulate the entire SD-WAN fabric through NETCONF access, rerouting traffic, altering configurations, and establishing persistence across wide-area networks.

- CVE-2026-20127 - CVSS: 10/10
- Authentication bypass vulnerability affects the peering authentication mechanism of two critical Cisco SD-WAN components:
 - Catalyst SD-WAN Controller (formerly SD-WAN vSmart)
 - Catalyst SD-WAN Manager (formerly SD-WAN vManage)

An unauthenticated, remote attacker can send crafted requests to a vulnerable device and bypass authentication entirely. Successful exploitation results in the attacker logging in as an internal, high-privileged, non-root user account. From there, they gain access to NETCONF, enabling full manipulation of network configuration across the SD-WAN fabric.

Attack Chain: Chaining Two Flaws

The U.S. Cybersecurity and Infrastructure Security Agency (CISA) added this zero-day and an older Cisco Catalyst SD-WAN bug, CVE-2022-20775, to its Known Exploited Vulnerabilities catalog. CISA issued Emergency Directive 26-03, giving federal agencies just two days to patch both vulnerabilities.

Threat actors have been chaining the two flaws to:

- Bypass authentication (using the new zero-day).
- Escalate privileges (using the older flaw).
- Establish persistence on compromised SD-WAN systems.

The Threat Actor: UAT-8616

Cisco Talos has attributed the attacks to UAT-8616, a "highly sophisticated cyber threat actor" that has been active since at least 2023. While not linked to any known threat group, the actor's capabilities and operational security point to a well-resourced, state-sponsored or advanced persistent threat operation.

Exploitation in the Wild

Cisco confirmed limited exploitation of this zero-day in active attacks. The company has released indicators of compromise to help organizations hunt for malicious activity targeting internet-exposed Catalyst SD-WAN systems.

Affected Deployments

The vulnerability affects all configurations of the impacted products across multiple deployment models:

- On-premises deployments
- Cisco-hosted SD-WAN Cloud
- Cisco-hosted SD-WAN Cloud (Cisco-managed)
- Cisco-hosted SD-WAN Cloud (FedRAMP environment)

Indicators of Compromise

- Cisco Catalyst SD-WAN Controller systems that are exposed to the internet and that have ports exposed to the internet are at risk of exposure to compromise.
- Customers are encouraged to audit the *auth.log* file, located at `/var/log/auth.log`, for entries that are related to **Accepted publickey for vmanage-admin** from unknown or unauthorized IP addresses, as shown in the following example:
 - `2026-02-10T22:51:36+00:00 vm sshd[804]: Accepted publickey for vmanage-admin from port [REDACTED PORT] ssh2: RSA SHA256:[REDACTED KEY]`
- Customers must check the IP address in the *auth.log* log file against the configured System IPs that are listed in the Cisco Catalyst SD-WAN Manager web UI in the **WebUI > Devices > System IP** column.
- For help determining if a Cisco Catalyst SD-WAN Controller or Cisco Catalyst SD-WAN Manager has been compromised, customers should open a case with the Cisco Technical Assistance Center (TAC). Before opening a new TAC case, customers are encouraged to issue the **request admin-tech** command from each of the control components in the SD-WAN deployment so that the *admin-tech* file can be provided to the Cisco TAC for review.

No Workarounds. Patch Now.

Cisco has released software updates addressing this vulnerability. There are no workarounds. Organizations must patch immediately.

Mitigation

- Apply Cisco's security updates to all affected Catalyst SD-WAN Controller and Manager instances without delay.

- Prevent access from unsecured networks. Protect SD-WAN control components behind firewalls.
- Filter traffic to allow only known, trusted hosts to communicate with these systems.
- Disable HTTP for the Catalyst SD-WAN Manager web UI administrator portal. Use HTTPS exclusively.
- Regularly monitor web logs for unexpected traffic to and from SD-WAN systems.
- Deploy SSL/TLS with certificates from a trusted certificate authority, or create self-signed certificates where appropriate.

Ready to see how AICenturion can secure you against AI risks?

Request a demo today: hello@cytex.io

Connect with our social media channels

