Active exploitation of Cisco Catalyst SD-WAN by UAT-8616

By Cisco Talos

Published: 2026-02-25 · Archived: 2026-04-05 14:16:53 UTC

Wednesday, February 25, 2026 11:13

Cisco Talos is tracking the active exploitation of CVE-2026-20127, a vulnerability in Cisco Catalyst SD-WAN Controller, formerly vSmart, that allows an unauthenticated remote attacker to bypass authentication and obtain administrative privileges on the affected system by sending a crafted request to an affected system. Successful exploitation may allow the attacker to gain administrative privileges on the Controller as an internal, high privileged, non-root, user account.

Talos clusters this exploitation and subsequent post-compromise activity as “UAT-8616” whom we assess with high confidence is a highly sophisticated cyber threat actor. After the discovery of active exploitation of the 0-day in the wild, we were able to find evidence that the malicious activity went back at least three years (2023). Investigation conducted by intelligence partners identified that the actor likely escalated to root user via a software version downgrade. The actor then reportedly exploited CVE-2022-20775 before restoring back to the original software version, effectively allowing them to gain root access.

UAT-8616's attempted exploitation indicates a continuing trend of the targeting of network edge devices by cyber threat actors looking to establish persistent footholds into high value organizations including Critical Infrastructure (CI) sectors.

Customers are strongly advised to follow the guidance published in the security advisories discussed below. Additional recommendations specific to Cisco are available here. Customers support is also available by initiating a TAC request. Talos strongly recommends that customers and partners using Cisco Catalyst SD-WAN technology follow the steps outlined in this advisory to help protect their environments.

Initial Peering Event Analysis

The initial and most critical activity to look for is any control connection peering event identified in Cisco Catalyst SD-WAN logs, as this may indicate an attempt at initial access via CVE-2026-20127. All such peering events require manual validation to confirm their legitimacy, with particular focus on vManage peering types. Threat actors who compromise Cisco Catalyst SD-WAN infrastructure often establish unauthorized peer connections that may appear superficially normal but occur at unexpected times, originate from unrecognized IP addresses, or involve device types inconsistent with the environment's architecture. A comprehensive review process is essential to distinguish between legitimate network operations and potential indicators of compromise.

Validation Checklist Items Include

- Verify the timestamp of each peering event against known maintenance windows, scheduled configuration changes, and normal operational hours for your environment.
- Confirm the public IP address corresponds to infrastructure owned or operated by your organization or authorized partners by cross-referencing against asset inventories and authorized IP ranges.
- Validate the peer system IP matches documented device assignments within your Cisco Catalyst SD-WAN topology.
- Review the peer type (vmanage, vsmart, vedge, vbond) to ensure it aligns with expected device roles in your deployment.
- Correlate multiple events from the same source IP or system IP to identify patterns of reconnaissance or persistent access attempts.
- Cross-reference event timing with authentication logs, change management records, and user activity to establish whether the connection was initiated by authorized personnel.

Sample Log Entry

> Feb 20 22:03:33 vSmart-01 VDAEMON_0[2571]: %Viptela-vSmart-VDAEMON_0-5-NTCE-1000001: control-connection-state-change new-state:up peer-type:vmanage peer-system-ip:1.1.1.10 public-ip:192.168.3.20 public-port:12345 domain-id:1 site-id:1005

Log Analysis

In the identified example, the peer-system-ip should be validated as matching the expected IP address schema in-use, the timestamp should be validated as matching any events which might cause a peering event to occur and the public-ip should be validated as being an expected source for a peering event.

Additional Investigative Guidance

The following may be high-fidelity indicators of a successful compromise by UAT-8616 in an SD-WAN infrastructure setup:

- Creation, usage and deletion of malicious user accounts including otherwise absent bash_history and cli-history.
- Interactive root sessions on production systems including unaccounted SSH keys, known hosts and bash history. For example:
    - Notification: system-login-change severity-level:minor host-name:"<node_name>" system-ip:<IP> user-name:""root""
    - SSH Keys in: /home/root/.ssh/authorized_keys with “PermitRootLogin” set to “yes” in /etc/ssh/sshd_config
    - Known hosts in: /home/root/.ssh/known_hosts
- Unauthorized or unaccounted SSH keys (“authorized_keys”) for the “vmanage-admin” account: /home/vmanage-admin/.ssh/authorized_keys/
- Abnormally small logs including absent or size 0/1/2 byte logs.
- Evidence of log and history clearing or truncation including:
    - syslog

    - wtmp
    - lastlog
    - cli-history
    - bash_history
    - Logs residing in /var/log/
- Presence of cli-history file for a user without the bash history.
- Indications of unexplained peers being dropped or added to the environment.
- Unexpected and unauthorized version downgrades and upgrades accompanied by a system reboot. For example (log entries):
    - Waiting for upgrade confirmation from user. Device will revert to previous software version <version> in '100' seconds unless confirmed.
    - Software upgrade not confirmed. Reverting to previous software version
- Evidence of exploitation of CVE-2022-20775 such as specially crafted username path traversal string (E.g. “/../../” or “/\n&../\n&../”).

Recommendations

We strongly recommend that you perform the steps outlined in this document. Cisco has also published a hardening guide for Cisco Catalyst SD-WAN deployments located at https://sec.cloudapps.cisco.com/security/center/resources/Cisco-Catalyst-SD-WAN-HardeningGuide. It is strongly recommended that any customers who are utilizing the Cisco Catalyst SD-WAN technology follow the guidance provided in this hardening guide. We also recommend referring to advisories here and here and the Cisco Catalyst SD-WAN threat hunting guide released by our intelligence partners for additional detection guidance.

Talos Coverage

Talos is releasing the following Snort coverage for this threat and associated vulnerability:

- 65938, 65958
