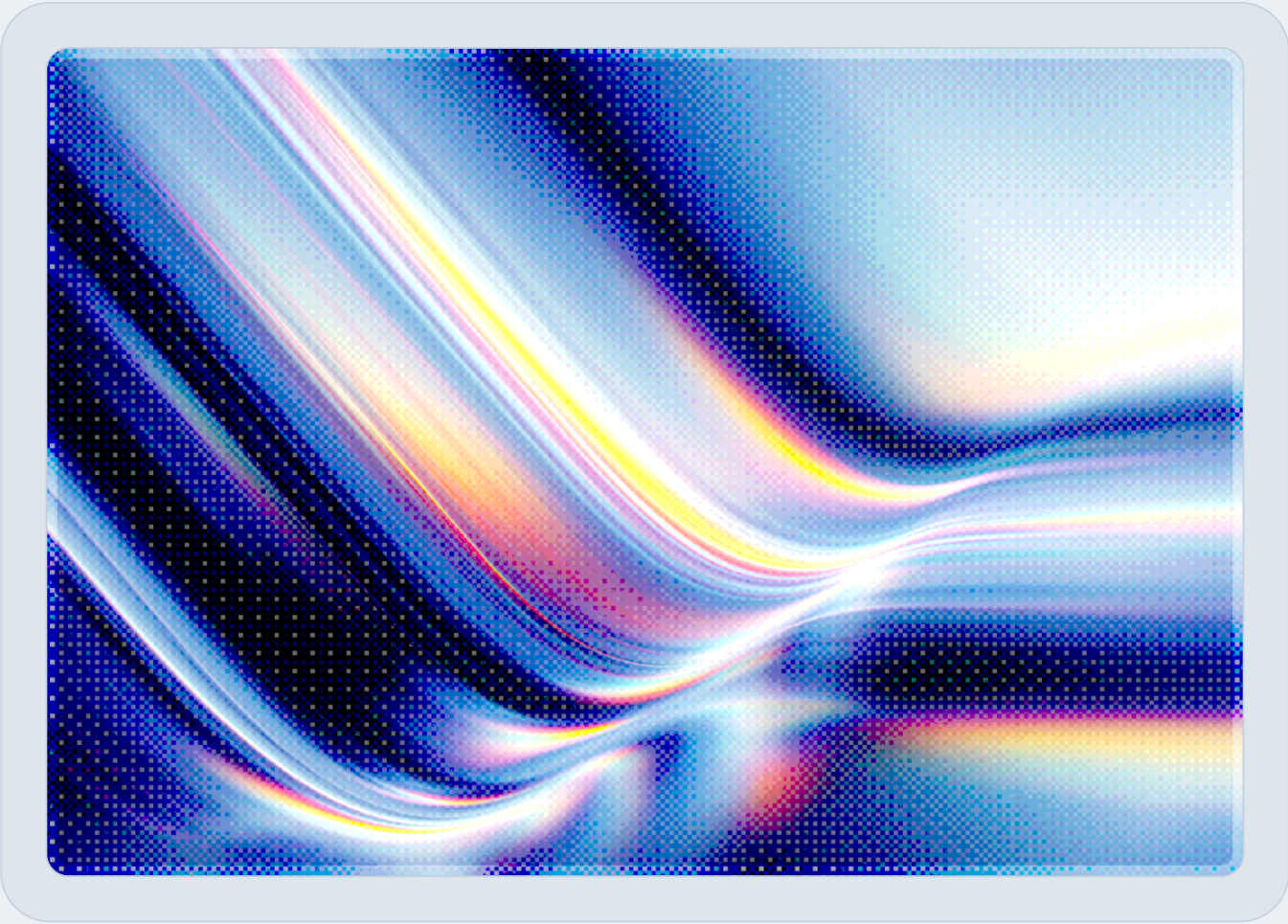
CSAI Foundation | Cloud Security Alliance

Cisco SD-WAN CVE-2026-20245 Zero-Day: Root Access Pre-Disclosure Exploitation

2026-06-27

AI-assisted Rapid Research



CSAI

CSA cloud security alliance®

Key Takeaways

- CVE-2026-20245 is a CVSS 7.8 (High) command injection flaw in Cisco Catalyst SD-WAN Manager, Controller, and Validator that allows an authenticated attacker with netadmin privileges to execute arbitrary commands as root via a crafted file upload, with no available workaround.
- Mandiant researchers discovered evidence of pre-disclosure exploitation dating to at least March 2026 — roughly three months before Cisco published the patch on June 4, 2026 — confirming the vulnerability was weaponized before defenders had any formal remediation path.
- The attack chain most likely combined two preceding authentication bypass flaws (CVE-2026-20127 or CVE-2026-20182) to achieve initial access, though Mandiant's investigation could not definitively confirm which specific flaw was used for initial entry [1]. That access was then leveraged to create a hidden root-level account (`troot` with UID 0), enabling persistent, unrestricted control of the management plane.
- Because Cisco Catalyst SD-WAN Manager controls configuration distribution across an entire SD-WAN fabric, a management plane compromise of this kind allows an attacker to push malicious configuration changes to every downstream edge device — not just the compromised controller node.
- The threat actor demonstrated operational sophistication — as assessed by Mandiant — through systematic anti-forensic cleanup [1]: pre-exploitation backups of system files, post-exploitation restoration, and targeted evidence deletion intended to obscure the intrusion from forensic investigators.
- No workaround exists. Immediate upgrade to patched releases is the sole remediation; organizations should preserve forensic state by running the `request admin-tech` command before initiating an upgrade.

Background

Cisco Catalyst SD-WAN is a widely deployed software-defined wide area network platform used by enterprises, managed service providers, and telecommunications carriers to centrally manage distributed branch and edge infrastructure. The architecture divides operational responsibilities among three control components: the SD-WAN Manager (formerly vManage) serves as the single-pane-of-glass management plane, the SD-WAN Controller (vSmart) handles routing policy and data plane programming, and the SD-WAN Validator (vBond) manages orchestration and device authentication. Because the Manager sits at the apex of this hierarchy and communicates directly with all other components, it represents the highest-value target in an SD-WAN deployment — an attacker who controls vManage effectively controls the entire network fabric.

CVE-2026-20245 is the seventh Cisco SD-WAN zero-day to be exploited in 2026 [1][4]. The pattern reflects a sustained adversarial interest in SD-WAN infrastructure that began materializing publicly in late 2025, when threat actors began probing authentication mechanisms in Cisco's control plane. CVE-2026-20127 and CVE-2026-20182, both authentication bypass vulnerabilities that allow unauthenticated remote attackers to gain administrative privileges, were exploited in earlier intrusions attributed with high confidence to threat cluster UAT-8616 [2][4]. CVE-2026-20245 represents a subsequent stage of that campaign: where the earlier flaws enabled unauthorized access, this vulnerability converted authenticated access into unrestricted root control.

Cisco published the security advisory for CVE-2026-20245 on June 4, 2026, describing it as a privilege escalation vulnerability resulting from insufficient validation of user-supplied input in the CLI's tenant-list upload feature [2]. The advisory was accompanied by patches across six active release trains. On June 24, 2026, Google Mandiant published a detailed technical analysis revealing that active exploitation had already occurred in the wild — well before the patch existed — targeting SD-WAN infrastructure at a service provider [1]. Mandiant researchers Chester Sng, Pete Boonyakarn, Logeswaran Nadarajan, and Lukasz Lamparski authored the analysis and were credited by Cisco PSIRT with discovering and reporting the vulnerability [1][2].

Security Analysis

Vulnerability Mechanics

The vulnerability resides in the `tenant-upload` command within the Cisco Catalyst SD-WAN Manager CLI. This feature, intended to allow administrators to provision tenant configurations in bulk via CSV file, fails to adequately validate user-supplied input before passing file contents to an underlying shell script. An attacker who can invoke this command — requiring at minimum `netadmin`-level CLI access — can embed arbitrary shell commands in a crafted CSV file and have them executed with root privileges [1][2].

The CVSS 3.1 base vector of `AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H` scores the vulnerability at 7.8, reflecting that local access with low privileges is sufficient and that no user interaction is required [2][3]. The high ratings across confidentiality, integrity, and availability reflect the full-system impact of root execution. The local attack vector (`AV:L`) might suggest limited exposure, but in practice an SD-WAN management plane is reachable via SSH and web interfaces that are in many deployments exposed to broad administrative networks or, in misconfigured environments, to the public internet — a configuration Cisco's SD-WAN hardening guidance explicitly warns against [2]. In the observed intrusion, the threat actor achieved the necessary CLI access through prior exploitation of remote authentication bypass vulnerabilities, effectively converting CVE-2026-20245 from a local privilege escalation into a networked root compromise.

The Observed Attack Chain

Mandiant's investigation reconstructed a multi-phase intrusion that unfolded over several months [1]. During late 2025 and early 2026, the attacker established unauthorized peering connections to SD-WAN Manager devices, most likely through exploitation of CVE-2026-20127 or CVE-2026-20182, which permit unauthenticated remote administrative access. These initial connections provided visibility into the target environment and likely facilitated the exfiltration of certificate material used in later phases.

By March 2026, the attacker had established more persistent footholds. Authentication via SSH as the `vmanage-admin` service account was observed, followed by modification of the default `admin` account password — which Mandiant assessed as a deliberate lockout intended to complicate defender response [1]. The attacker then uploaded a malicious CSV file named `evil_tenant.csv` and invoked the privilege escalation:

```
request tenant-upload tenant-list /home/admin/evil_tenant.csv vpn 0
```

The payload embedded in the CSV executed shell commands that appended a new entry to `/etc/passwd` and `/etc/shadow` – creating the account `troot` with UID 0 (root) and a pre-set password hash. Before executing the payload, the attacker copied the original `/etc/passwd` and `/etc/shadow` files to hidden backup locations, enabling restoration of the originals after exploitation. This backup-and-restore behavior is consistent with a deliberate anti-forensic technique: by restoring the original files after use, the attacker ensures modified system files exist only transiently, reducing the probability that passive log collection captures evidence of account injection [1].

The `troot` account was subsequently accessed via the `su` command from the `admin` session, granting unrestricted root shell access. The threat actor then used this access to make configuration changes before systematically reversing them and deleting created files – running verification scripts to confirm that evidence had been eliminated [1].

Management Plane Compromise and Network-Wide Impact

The strategic significance of a vManage compromise extends well beyond the compromised node itself. Cisco SD-WAN Manager is the authoritative source of truth for device configuration across the entire SD-WAN fabric; when a configuration change is committed and pushed, it propagates to all enrolled edge devices – WAN routers, branch gateways, and data center edge nodes – without requiring authentication at each endpoint beyond the trust relationship with the manager. Mandiant observed at least one case in which the threat actor pushed a configuration change to edge devices following management plane compromise [1]. This single observed instance illustrates a central risk of management plane compromise: an attacker with root access to vManage can, in principle, alter routing policy, redirect traffic, introduce rogue certificate authorities, degrade encryption parameters, or establish persistent backdoors on every device the manager controls.

This consequence is not unique to CVE-2026-20245; it is an architectural property of centralized management planes. However, CVE-2026-20245 lowers the bar for reaching that plane by providing a root escalation path accessible to any authenticated CLI user. The combination of low privilege requirements, no workaround, and high-value management plane position makes this vulnerability operationally more dangerous than its CVSS score alone conveys.

Threat Actor Profile

Attribution of this specific intrusion remains incomplete. The exploitation of preceding SD-WAN authentication bypass vulnerabilities has been publicly clustered under the designation UAT-8616, a sophisticated actor active since at least 2023 that focuses on network appliance compromise as an initial access mechanism [4]. The operational tradecraft observed in the CVE-2026-20245 intrusion — rogue peering connections, credential manipulation, anti-forensic cleanup, and a deliberate backup-and-restore pattern — is consistent with a state-nexus or highly capable criminal actor rather than opportunistic exploitation. However, no formal attribution to UAT-8616 or any named threat group has been published for the CVE-2026-20245 activity as of this writing.

The targeting of a service provider's SD-WAN infrastructure is characteristic of a campaign seeking broad, persistent access to downstream customer networks rather than a single-organization intrusion. Service providers that operate managed SD-WAN services on behalf of enterprise customers should consider any compromise of their management plane as a potential supply chain intrusion affecting all managed tenants.

Recommendations

Immediate Actions

Organizations running Cisco Catalyst SD-WAN Manager, Controller, or Validator must prioritize upgrading to a patched release. Cisco has confirmed no workaround is available; the vulnerability can only be remediated through software update [2]. Fixed versions by release train are: 20.9.9.2, 20.12.7.2, 20.15.4.5, 20.15.5.3, 20.18.3.1, and 26.1.1.2 [1][2]. CVE-2026-20245 was added to CISA's Known Exploited Vulnerabilities Catalog on June 9, 2026 [3], reinforcing the urgency of immediate remediation. Before initiating an upgrade, administrators should execute the `request admin-tech` command on all control-plane components to capture a complete diagnostic bundle; this bundle preserves log state that may be overwritten during the upgrade process and is essential for any subsequent forensic investigation [1][2].

Administrators should also immediately conduct threat hunting against all SD-WAN management nodes using the indicators published by Mandiant [1]. Mandiant identifies the following as high-fidelity indicators [1]: the presence of the file `/home/admin/evil_tenant.csv` (SHA256: `b82936f37648518425c7d3cf9e09eaffa41d7cdb3840f6a40287e3a108880f7b`), the existence of a `troot` account in `/etc/passwd` or `/etc/shadow`, and entries in

`/var/log/auth.log` showing `su` escalation to `troot`. Execution of the script `vconfd_script_upload_tenant_list.sh` outside of legitimate administrative workflows should also be treated as a high-fidelity indicator of exploitation [1]. The Mandiant report includes a detection script that can be run directly against affected devices to check for these artifacts. Network indicators — specifically the IP addresses `126.51.108[.]152`, `76.92.245[.]217`, `207.190.37[.]94`, and five additional addresses documented in the Google Cloud blog post — should be evaluated against firewall, VPN, and SSH access logs [1].

Short-Term Mitigations

Prior to patching, or where patching timelines must be sequenced carefully across a large deployment, organizations should implement compensating controls focused on reducing the privilege escalation path. Access to the SD-WAN Manager CLI should be restricted to a named allowlist of authorized administrator workstations and jump hosts; any authentication from outside that allowlist should generate an immediate alert [2]. Multi-factor authentication should be enforced on all accounts capable of reaching the CLI, including service accounts used by automation pipelines. The `vmanage-admin` account — which was the initial SSH target in the observed intrusion — should be reviewed for necessity; if it is not required for operational purposes, it should be disabled or its SSH key material rotated immediately.

Network segmentation controls should be audited to confirm that the SD-WAN Manager's management interface is not reachable from internet-facing or untrusted network segments. Cisco's SD-WAN hardening guidance recommends isolating the Manager's VPN 512 management interface into a dedicated internal management VLAN [2]. Organizations that have not implemented this isolation should treat it as an urgent remediation item independent of patching status. Additionally, all current SD-WAN Manager configuration snapshots should be preserved offline so that any unauthorized configuration changes can be detected through diff analysis.

Strategic Considerations

The sustained exploitation of Cisco SD-WAN vulnerabilities in 2026 underscores a structural risk in centralized management plane architectures: the management plane is both the most powerful component of the network and, in many observed deployments, the least consistently hardened. A Zero Trust approach to management plane access — in which every administrative session is verified against identity, device posture, and contextual signals — reduces reliance on implicit network trust and constrains the lateral movement available to an attacker who compromises a single credential. CSA's

Zero Trust guidance articulates this principle directly: control plane access decisions should be based on cryptographically verified identity and continuous session validation, not implicit trust derived from network position [5].

Service providers operating managed SD-WAN environments on behalf of enterprise customers should reassess whether their management plane architecture adequately isolates tenant management domains. A compromise of a shared vManage instance — as described in the Mandiant report — may constitute a data breach or service compromise affecting multiple downstream customers, with associated notification and contractual obligations. Organizations should also evaluate whether their current monitoring posture would have detected the behavior described here: the observed intrusion employed techniques consistent with a deliberate effort to evade passive log collection, suggesting that real-time behavioral monitoring at the management plane is a necessary complement to log aggregation.

CSA Resource Alignment

This incident maps directly to several domains within CSA's established frameworks. The Cloud Controls Matrix (CCM v4.0) addresses the relevant controls under the Infrastructure and Virtualization Security (IVS) domain, which establishes requirements for network segmentation, management plane isolation, and vulnerability patching cadence [6]. The IVS controls for network architecture (IVS-06) and configuration management (IVS-10) are directly applicable to SD-WAN management plane hardening. CCM's Identity and Access Management (IAM) domain covers the principle of least-privilege access that would have constrained the exploitation path described here.

CSA's Zero Trust guidance provides the architectural framing for a durable response to this class of vulnerability. As documented in CSA's guidance on achieving operational resilience through Zero Trust, the management plane of any network infrastructure should be treated as a high-value target requiring continuous verification rather than implicit trust [7]. The principle that "the control plane defines what is actually allowed" is precisely why adversaries invest in management plane compromise: subvert the policy engine and you subvert the network. CSA's Zero Trust Cloud Control Plane guidance published in January 2026 emphasizes that isolation, private endpoints, and microsegmentation are necessary but insufficient without continuous session validation [5] — a prescription that applies with equal force to on-premises SD-WAN management infrastructure.

The MAESTRO threat modeling framework, developed by CSA for agentic AI architectures, offers a transferable conceptual lens for SD-WAN architects, even though the framework was designed for AI systems. MAESTRO's treatment of how privileged management interfaces become high-value attack

targets — and how lateral movement from a management node can propagate configuration changes to all downstream agents — is applicable to SD-WAN deployments as well. Security architects reviewing management plane access controls will find MAESTRO's analysis of trust hierarchies and privileged plane isolation relevant to their work.

References

[1] Sng, Chester, Pete Boonyakarn, Logeswaran Nadarajan, and Lukasz Lamparski (Mandiant/Google). "Zero-Day Exploitation of Vulnerability (CVE-2026-20245) in Cisco Catalyst SD-WAN Manager." Google Cloud Blog, June 24, 2026.

[2] Cisco PSIRT. "Cisco Catalyst SD-WAN Controller, Catalyst SD-WAN Manager, and Catalyst SD-WAN Validator Authenticated Privilege Escalation Vulnerability." Cisco Security Advisory cisco-sa-sdwan-privesc-4uxFrdzx, June 4, 2026.

[3] NIST National Vulnerability Database. "CVE-2026-20245 Detail." NVD, 2026.

[4] Kovacs, Eduard. "Cisco SD-WAN Zero-Day Exploited Months Before Patching." SecurityWeek, June 25, 2026.

[5] Cloud Security Alliance. "Zero Trust in the Cloud: Designing Security Assurance at the Control Plane." CSA Blog, January 30, 2026.

[6] Cloud Security Alliance. "Cloud Controls Matrix v4.0." CSA, 2021.

[7] Cloud Security Alliance. "Zero Trust Guidance for Achieving Operational Resilience." CSA, April 6, 2026.