INTELLIGENCE BRIEFING
Security Command Center
TLP:CLEAR
2026-06-06 14:05 UTC

Arista Networks EOS - Arista EOS Unexpected Tunnel Protocol Decapsulation and Forwarding Bypass

CVE VULNERABILITY | **HIGH** | CVSS 8.2 | **CISA KEV**

SCC Item ID	SCC-CVE-2026-0269
Type	CVE Vulnerability
CVE ID	CVE-2026-7473
Severity	HIGH
CVSS Base Score	8.2
EPSS Score	0.0003 (9th percentile)
KEV Status	Yes — CISA Known Exploited Vulnerability
Affected Products	Arista Networks EOS (platforms with VXLAN, decap-group, or GRE tunnel interface configurations)
Published	2026-06-05T00:00:00Z
Discovery Source	Vulncheck Kev

Executive Summary

A confirmed-exploited vulnerability in Arista Networks EOS allows attackers to bypass network segmentation by sending tunneled packets that the switch processes without verifying the tunnel protocol type. Any Arista EOS deployment using VXLAN, decap-groups, or GRE tunnel interfaces is at risk. Active exploitation is confirmed by both CISA and VulnCheck KEV listings, meaning threat actors are already using this flaw to move laterally across supposedly isolated network segments.

Technical Analysis

CVE-2026-7473 is a confirmed-exploited flaw in Arista EOS affecting platforms configured with tunnel decapsulation, VXLAN, decap-groups, or GRE tunnel interfaces. The root cause (CWE-284: Improper Access Control; CWE-693: Protection Mechanism Failure) is the absence of tunnel protocol type verification. When a packet's destination IP matches a configured decapsulation IP, EOS decapsulates and forwards it regardless of whether the encapsulating protocol was explicitly configured. An attacker with network access can craft tunneled packets to bypass segmentation controls, inject traffic into isolated segments, or manipulate forwarding paths. MITRE techniques mapped: T1021 (Remote Services), T1572 (Protocol Tunneling), T1599 (Network Boundary

Bridging), T1599.001 (Network Address Translation Traversal). CVSS base score: 8.2 (High), assessed by NIST NVD. Vendor CVSS score is not yet available. Listed in CISA KEV and VulnCheck KEV, confirming in-the-wild exploitation. Affected scope is limited to EOS platforms with tunnel decapsulation configurations present; platforms without these configurations are not affected by this specific bypass path.

Action Checklist

1. Step 1: Containment. Identify all Arista EOS devices in your environment with VXLAN, decap-group, or GRE tunnel interface configurations. Audit running configs using 'show running-config' for 'decap-group', 'tunnel interface', or 'vxlan' stanzas. Temporarily restrict inbound tunneled traffic at upstream perimeter controls (firewall ACLs or IPS rules) to known, authorized sources until patching is complete. Prioritize internet-adjacent or inter-segment EOS devices.
2. Step 2: Detection. Review EOS syslog and packet capture data for unexpected decapsulation events: tunnel traffic arriving from unauthorized sources, unexpected inter-VLAN or inter-segment forwarding, or traffic matching decap IPs from hosts that should have no tunnel relationship. Query SIEM for anomalous flows to/from EOS management and data-plane IPs. Cross-reference with NIST AU-6 (Audit Record Review) requirements, look for forwarding anomalies in NetFlow or sFlow data if enabled. No public IOC hashes or IPs are confirmed in the current source data.
3. Step 3: Eradication. Retrieve the full Arista Security Advisory (advisories.arista.com) to confirm exact affected EOS version ranges and corresponding patches before applying updates. Apply the Arista-published patch for CVE-2026-7473 per the official advisory. Where patching is not immediately possible, remove unused tunnel decapsulation configurations (VXLAN, decap-groups, GRE) as a temporary mitigation if those features are not operationally required.
4. Step 4: Recovery. After patching, validate that tunnel protocol type verification is enforced by testing with crafted non-configured protocol packets and confirming they are dropped. Re-enable any temporarily restricted tunnel traffic from authorized sources. Monitor EOS forwarding tables and syslog for residual anomalies for at least 72 hours post-remediation. Verify audit logging per NIST AU-2 and CIS 8.2 is capturing tunnel decapsulation events.
5. Step 5: Post-Incident. This vulnerability exposes a control gap in protocol-level verification at network enforcement points. Review segmentation architecture to ensure network boundaries do not rely solely on device-level tunnel configuration for enforcement. Map findings against NIST AC-4 (Information Flow Enforcement) and AC-3 (Access Enforcement), verify that segmentation policy is enforced at multiple layers, not only at the EOS platform. Document lessons learned and update network device configuration hardening standards per CIS 4.2 (Secure Configuration Process for Network Infrastructure).

IR / Forensic Enrichment

Triage Priority	IMMEDIATE
Escalation Criteria	Escalate immediately to senior IR leadership and legal/compliance if NetFlow, sFlow, or MAC table evidence confirms that tunnel bypass traffic successfully reached network segments containing regulated data (PII, PHI, PCI card data), or if any EOS device shows a decap-group or tunnel interface entry not present in the authorized configuration baseline, indicating potential attacker-injected configuration persistence.

Recovery Notes	After patching all affected EOS devices to the Arista-confirmed remediated version, conduct crafted-packet validation testing (Scapy or equivalent) against each patched device to confirm protocol type verification is enforced before re-enabling any temporarily restricted tunnel traffic from authorized peers. Monitor EOS syslog, 'show mac address-table dynamic', and NetFlow data continuously for a minimum of 72 hours post-patch, specifically filtering for any inter-segment forwarding events in VLANs or VRFs that were previously isolated by tunnel configuration — residual anomalies during this window may indicate attacker persistence through sessions established prior to containment. Re-baseline all EOS device running configurations against a clean hardening standard that explicitly prohibits unconfigured or unused decap-group and tunnel interface stanzas.
Forensic Artifacts	EOS syslog buffer ('show logging') filtered for decapsulation events, unexpected forwarding decisions, or tunnel-related error messages — the primary artifact for reconstructing the protocol bypass exploitation timeline on Arista EOS | Full packet captures (pcap) of UDP/4789 (VXLAN) and GRE protocol 47 traffic on affected switch uplinks, preserving both outer tunnel headers and inner encapsulated payloads — required to document which inner source/destination pairs were forwarded across segment boundaries without authorized tunnel relationships | NetFlow or sFlow records from the collection point covering EOS data-plane IPs for the 30 days prior to detection — used to identify the earliest unauthorized tunnel source IP communicating with EOS decap-group addresses, establishing attacker dwell time | 'show mac address-table dynamic' and 'show ip route' outputs timestamped at detection and at 24-hour intervals — unexpected MAC entries or routes in isolated VLANs/VRFs are direct forensic indicators of successful lateral movement achieved via the CVE-2026-7473 bypass mechanism | Full 'show running-config' and 'show startup-config' snapshots from all affected EOS devices captured before any remediation action — these document the exact decap-group, VXLAN VNI, and GRE tunnel interface configurations that were present during exploitation, and serve as the authoritative record for scope determination and regulatory reporting

Per-Action IR Details

Step 1: Containment — Identify all Arista EOS devices in your environment with VXLAN, decap-group, or GRE tunnel interface configurations. Audit running configs using 'show running-config' for 'decap-group', 'tunnel interface', or 'vxlan' stanzas. Temporarily restrict inbound tunneled traffic at upstream perimeter controls (firewall ACLs or IPS rules) to known, authorized sources until patching is complete. Prioritize internet-adjacent or inter-segment EOS devices.

NIST Phase: Containment

Reference: NIST 800-61r3 §3.3 — Containment Strategy

Controls: NIST AC-4 (Information Flow Enforcement), NIST AC-6 (Least Privilege), CIS 4.4 (Implement and Manage a Firewall on Servers), CIS 1.1 (Establish and Maintain Detailed Enterprise Asset Inventory)

Compensating: Run 'show running-config | grep -E "decap-group|tunnel|vxlan"' via SSH against each EOS device in sequence using a simple bash loop: 'for host in $(cat eos_hosts.txt); do ssh admin@$host "show running-config | grep -E decap-group\|tunnel\|vxlan"; done'. Pipe results to a file for triage. Use upstream firewall (pfSense, iptables, or Cisco ACL) to block inbound UDP/4789 (VXLAN) and GRE (protocol 47) from all sources not in an explicit allow-list — this is achievable by a 2-person team in under an hour without a SIEM.

Evidence: Before modifying any ACL or config, capture: (1) 'show running-config' full output from each EOS device showing existing decap-group, tunnel, and vxlan stanzas; (2) 'show interfaces' output to document active tunnel interface states; (3) 'show ip route' and 'show mac address-table' to baseline current forwarding state; (4) upstream firewall session tables showing established tunnel sessions at the time of discovery — these pre-containment states document attacker-established tunnel relationships that may otherwise be lost when ACLs are applied.

Step 2: Detection — Review EOS syslog and packet capture data for unexpected decapsulation events: tunnel traffic arriving from unauthorized sources, unexpected inter-VLAN or inter-segment forwarding, or traffic matching decap IPs from hosts that should have no tunnel relationship. Query SIEM for anomalous flows to/from EOS management and data-plane IPs. Cross-reference with NIST AU-6 (Audit Record Review) requirements — look for forwarding anomalies in NetFlow or sFlow data if enabled. No public IOC hashes or IPs are confirmed in the current source data.

NIST Phase: Detection Analysis

Reference: NIST 800-61r3 §3.2 — Detection and Analysis

Controls: NIST AU-6 (Audit Record Review, Analysis, And Reporting), NIST AU-2 (Event Logging), NIST AU-3 (Content Of Audit Records), CIS 8.2 (Collect Audit Logs)

Compensating: Without a SIEM, collect EOS syslog to a central rsyslog server and grep for decapsulation-related messages: 'grep -E "decap|tunnel|vxlan|GRE|unexpected.*forward" /var/log/eos-syslog.log'. Simultaneously run a targeted Wireshark/tcpdump capture on the uplink port of each affected EOS device: 'tcpdump -i eth0 -w eos_tunnel_capture.pcap "(udp port 4789) or (proto 47)"' — filter captures in Wireshark using display filter 'vxlan || gre' and manually inspect for inner packets sourced from segments that should have no tunnel relationship with the destination. Correlate against 'show ip route' changes and 'show logging' on EOS for route or MAC table anomalies.

Evidence: Before querying logs, preserve: (1) EOS syslog buffer output via 'show logging' — specifically filter for tunnel decapsulation events and unexpected forwarding decisions; (2) NetFlow or sFlow records from the collection point covering the EOS data-plane IPs for the 30 days prior to detection — look for flows where outer tunnel source IPs do not match the authorized decap-group peer list defined in 'show running-config'; (3) full packet captures (pcap) of UDP/4789 and GRE protocol 47 traffic on affected segments, preserving both outer and inner header layers to document the bypass mechanism; (4) 'show arp' and 'show mac address-table dynamic' outputs timestamped at detection — unexpected MACs or ARP entries in isolated VLANs indicate successful lateral movement via the bypass.

Step 3: Eradication — Apply the Arista-published patch for CVE-2026-7473 per the official Arista Security Advisory. Note: specific patched EOS version numbers are not confirmed in the current source data — retrieve the authoritative advisory directly from Arista's Security Advisories page (advisories.arista.com) before applying updates. Where patching is not immediately possible, remove unused tunnel decapsulation configurations (VXLAN, decap-groups, GRE) as a temporary mitigation if those features are not operationally required.

NIST Phase: Eradication

Reference: NIST 800-61r3 §3.4 — Eradication

Controls: NIST SI-2 (Flaw Remediation), CIS 7.3 (Perform Automated Operating System Patch Management), CIS 7.4 (Perform Automated Application Patch Management), CIS 7.1 (Establish and Maintain a Vulnerability Management Process), CIS 7.2 (Establish and Maintain a Remediation Process)

Compensating: For teams without automated patch management, script the EOS upgrade sequence: (1) download the validated EOS .swi image from Arista's portal to a staging server; (2) SCP to each device: 'scp EOS-.swi admin@:/mnt/flash/'; (3) set boot image: 'boot system flash:EOS-.swi' then reload; (4) verify post-upgrade with 'show version'. For temporary config-based mitigation on devices that cannot be patched immediately, remove decap-group stanzas with 'no decap-group ' and remove unused tunnel interfaces with 'no interface Tunnel' — document every removed stanza in a change record so it can be restored if operationally required post-patch.

Evidence: Before applying the patch or removing tunnel configs, capture: (1) full 'show running-config' and 'show startup-config' from every affected EOS device to document pre-patch state and serve as rollback reference; (2) 'show version' output confirming the vulnerable EOS version number for documentation and regulatory reporting; (3) 'show interfaces Tunnel' and 'show decap-group' outputs to record which tunnel configurations were active at time of eradication — these are required for post-incident root cause analysis to determine if unauthorized decap-group entries were injected or pre-existing misconfiguration was exploited.

Step 4: Recovery — After patching, validate that tunnel protocol type verification is enforced by testing with crafted non-configured protocol packets and confirming they are dropped. Re-enable any temporarily

restricted tunnel traffic from authorized sources. Monitor EOS forwarding tables and syslog for residual anomalies for at least 72 hours post-remediation. Verify audit logging per NIST AU-2 and CIS 8.2 is capturing tunnel decapsulation events.

NIST Phase: Recovery

Reference: NIST 800-61r3 §3.5 — Recovery

Controls: NIST AU-2 (Event Logging), NIST AU-12 (Audit Record Generation), CIS 8.2 (Collect Audit Logs), CIS 4.2 (Establish and Maintain a Secure Configuration Process for Network Infrastructure)

Compensating: Use Scapy (free, Python-based) to craft and send mismatched tunnel protocol packets to the patched EOS device from an authorized test host: construct a GRE-encapsulated packet where the inner protocol does not match a configured decap-group entry and confirm via 'show interfaces counters' that the packet is dropped rather than forwarded. Use 'show logging last 100' on EOS immediately after the test to verify a drop or error log entry is generated. Re-enable firewall ACLs for authorized tunnel sources incrementally — one peer at a time — and confirm each via 'show ip route' that only expected routes reappear, preventing accidental re-admission of attacker-controlled sources.

Evidence: During recovery, preserve: (1) Scapy or equivalent test packet crafting scripts and their output logs as validation evidence that CVE-2026-7473 is no longer exploitable on patched devices; (2) 'show version' post-patch confirming the remediated EOS build is running; (3) 72-hour rolling syslog captures post-patch filtered for any decapsulation events, unexpected VLAN crossing, or MAC table changes in previously isolated segments — these confirm no residual attacker persistence via pre-established tunnel sessions; (4) 'show ip route' and 'show mac address-table' snapshots at 0, 24, 48, and 72 hours post-patch to detect any unexpected forwarding re-emergence.

Step 5: Post-Incident — This vulnerability exposes a control gap in protocol-level verification at network enforcement points. Review segmentation architecture to ensure network boundaries do not rely solely on device-level tunnel configuration for enforcement. Map findings against NIST AC-4 (Information Flow Enforcement) and AC-3 (Access Enforcement) — verify that segmentation policy is enforced at multiple layers, not only at the EOS platform. Document lessons learned and update network device configuration hardening standards per CIS 4.2 (Secure Configuration Process for Network Infrastructure).

NIST Phase: Post Incident

Reference: NIST 800-61r3 §4 — Post-Incident Activity

Controls: NIST AC-4 (Information Flow Enforcement), NIST AC-3 (Access Enforcement), CIS 4.2 (Establish and Maintain a Secure Configuration Process for Network Infrastructure), CIS 7.1 (Establish and Maintain a Vulnerability Management Process), CIS 2.2 (Ensure Authorized Software is Currently Supported)

Compensating: Without a commercial network segmentation tool, conduct a manual architectural review using exported 'show running-config' outputs from all EOS devices — map every decap-group, VXLAN VNI, and GRE tunnel peer against a network diagram to identify segments where EOS is the sole enforcement boundary with no upstream or downstream ACL backup. Document each single-point-of-enforcement segment as a finding. Use osquery on hosts within those segments to validate that host-based firewall rules (iptables, Windows Firewall) are independently enforcing inter-segment access policy independent of EOS tunnel configurations. Update EOS device hardening checklist to include 'no unused decap-group or tunnel interface stanzas' as a required configuration baseline item.

Evidence: For the lessons-learned record, assemble: (1) timeline of attacker dwell time reconstructed from syslog, NetFlow, and MAC table change records — specifically how long unauthorized decapsulation-based lateral movement occurred before detection; (2) a segment impact map identifying which VLANs, VRFs, or security zones were reachable via the bypass, to scope potential data exposure for any required breach notification assessment; (3) pre- and post-incident 'show running-config' diffs for all affected EOS devices showing which tunnel configs were present, removed, or patched; (4) documentation of any regulated data (PII, PHI, PCI-scoped) resident in network segments that were accessible via the tunnel bypass — required for regulatory impact assessment.

Detection Guidance

Focus detection on unexpected decapsulation activity and anomalous cross-segment forwarding on EOS devices with tunnel configurations. Key sources: EOS syslog, NetFlow/sFlow records, and upstream firewall session logs. Look for: (1) tunnel traffic (UDP 4789 for VXLAN, IP protocol 47 for GRE) arriving at EOS decap IPs from hosts not in your authorized tunnel peer list; (2) traffic appearing in network segments it has no legitimate path to reach; (3) unexpected increases in decapsulated packet counts on EOS interfaces. NIST AU-6 (Audit Record Review) mandates regular review of these logs for exactly this type of anomaly. CIS 8.2 (Collect Audit Logs) requires audit logging to be enabled across enterprise assets, verify EOS syslog forwarding to your SIEM is active. No confirmed public IOC hashes, IPs, or domains are available in the current source data; do not treat absence of known IOCs as absence of exploitation.

Framework Mappings

MITRE-ATTACK

- **T1021** — Remote Services
- **T1572** — Protocol Tunneling
- **T1599** — Network Boundary Bridging
- **T1599.001** — Network Address Translation Traversal

NIST-800-53R5

- **AC-17** — Remote Access
- **AC-3** — Access Enforcement
- **CM-7** — Least Functionality
- **IA-2** — Identification and Authentication (Organizational Users)
- **IR-5** — Incident Monitoring

OWASP-TOP10-2021

- **A01:2021** — Broken Access Control

CIS-V8

- **6.1** — Establish an Access Granting Process
- **6.2** — Establish an Access Revoking Process

SOC2-TSC

- **CC6.1** — The entity implements logical access security software, infrastructure, and architectures over protected information assets

HIPAA-SECURITY

- **164.312(a)(1)** — Access Control

ISO-27001-2022

- **A.8.8** — Management of technical vulnerabilities

NIST-CSF-2

- **DE.AE-08** — Incidents are declared when adverse events meet the defined incident criteria

MITRE ATT&CK Mapping

Technique ID	Technique Name	Tactic
T1021	Remote Services	Lateral-Movement
T1572	Protocol Tunneling	Command-And-Control
T1599	Network Boundary Bridging	Defense-Evasion
T1599.001	Network Address Translation Traversal	Defense-Evasion

Sources

Source	URL	Tier
vulncheck_kev	https://nvd.nist.gov/vuln/detail/CVE-2026-7473	T1
CVE-2026-27473 Detail - NVD	https://nvd.nist.gov/vuln/detail/CVE-2026-27473	T1
CVE-2026-7473 - Exploits & Severity - Feedly	https://feedly.com/cve/CVE-2026-7473	T3
CVE-2026-39473: Simple History Information Disclosure Flaw	https://www.sentinelone.com/vulnerability-database/cve-2026-39473/	T3
CVE-2026-7473 - CVE Record	https://www.cve.org/CVERecord?id=CVE-2026-7473	T3
CISA KEV	https://www.cisa.gov/known-exploited-vulnerabilities-catalog	T1

Generated 2026-06-06 14:05 UTC by TJS Security Command Center