INTELLIGENCE BRIEFING
Security Command Center
TLP:CLEAR
2026-05-21 06:58 UTC

CVE-2024-12802: SonicWall Gen6 MFA Bypass Actively Exploited Despite Patched Firmware, Incomplete Remediation Creates Hidden Attack Surface

CVE VULNERABILITY | **CRITICAL** | CVSS 9.5

SCC Item ID	SCC-CVE-2026-0203
Type	CVE Vulnerability
CVE ID	CVE-2024-12802
Severity	CRITICAL
CVSS Base Score	9.5
EPSS Score	0.0006 (19th percentile)
Affected Products	SonicWall Gen6 SSL-VPN appliances (EOL April 16, 2026); Gen7 and Gen8 devices mitigated via firmware update alone
Published	2026-05-20T17:19:17
Discovery Source	Rss

Executive Summary

A critical authentication bypass vulnerability in SonicWall Gen6 SSL-VPN appliances is actively exploited, allowing attackers to log in without a second authentication factor even on patched devices where a required LDAP reconfiguration step was not completed. Confirmed active exploitation between February and March 2026 targets organizations across multiple sectors, with attack patterns consistent with initial access brokers positioning for ransomware deployment. Organizations running Gen6 appliances face an elevated and compounding risk: the firmware patch alone does not close the attack surface, and incomplete remediation is difficult to detect through standard log review.

Technical Analysis

CVE-2024-12802 (CVSS 9.5) is a dual-classification authentication bypass affecting SonicWall Gen6 SSL-VPN appliances, assigned CWE-287 (Improper Authentication) and CWE-306 (Missing Authentication for Critical Function). The vulnerability resides in the UPN (User Principal Name) login path, which fails to enforce MFA requirements. An attacker authenticating via UPN format bypasses the MFA gate entirely while producing log entries that appear visually consistent with a normal MFA-protected session, creating a detection blind spot.

Exploitation requires valid credentials, which threat actors obtain via pre-exploitation brute-forcing (T1110) before using the UPN path to authenticate without the second factor (T1556). Post-authentication behavior observed by ReliaQuest includes Cobalt Strike beacon deployment (T1587.001), BYOVD driver loading to disable EDR (T1543/T1562.001), lateral movement via RDP (T1021.001), and attacker infrastructure routed through VPS/VPN services (T1090, T1583.003). Remediation for Gen6 devices requires two steps: firmware update AND LDAP reconfiguration to enforce MFA on the UPN login path. Gen7 and Gen8 devices require firmware update only. Gen6 devices reach end-of-life April 16, 2026. NVD entry: https://nvd.nist.gov/vuln/detail/CVE-2024-12802 (T1 source, verified in item data).

Action Checklist

1. Step 1: Containment. Identify all SonicWall Gen6 SSL-VPN appliances in your environment. Restrict internet-facing VPN access to known IP ranges or place devices behind a WAF/IPS while remediation is completed. For Gen6 devices still in support, verify firmware has been updated to the patched version per SonicWall's advisory. Note: firmware update alone does not remediate the vulnerability on Gen6 appliances; LDAP reconfiguration (Step 3) is required. Reference NIST CM-7 (Least Functionality) and CIS 4.4 (Implement and Manage a Firewall on Servers).
2. Step 2: Detection. Review SSL-VPN authentication logs for logins using UPN format (user@domain.tld) rather than standard username format, particularly from unfamiliar source IPs or VPS/VPN infrastructure ranges. Correlate against SIEM for sessions where MFA was not challenged despite MFA policy being active. Flag any successful UPN-format authentications occurring during off-hours or from geolocations inconsistent with your workforce. Reference NIST AU-6 (Audit Record Review, Analysis, and Reporting) and CIS 8.2 (Collect Audit Logs). Apply D3-LAM (Local Account Monitoring) to identify anomalous account activity post-authentication.
3. Step 3: Eradication. Apply the SonicWall firmware patch for CVE-2024-12802. Then immediately complete the required LDAP reconfiguration step per SonicWall guidance to enforce MFA on the UPN login path. For Gen6 devices reaching end-of-life April 16, 2026, begin hardware replacement planning immediately. Reference NIST SI-4 (System Monitoring) and CIS 6.4 (Require MFA for Remote Network Access).
4. Step 4: Recovery. After completing both remediation steps, validate that UPN-format authentication attempts now trigger MFA challenges. Test from a controlled non-production test account using UPN login format and confirm MFA is enforced. Review authentication logs for the prior 60 days for any successful UPN-format logins that bypassed MFA. Treat any such session as a confirmed compromise and initiate incident response. Monitor for Cobalt Strike indicators, new scheduled tasks, and unexpected driver loads. Reference NIST CP-10 (System Recovery and Reconstitution) and D3-CRO (Credential Rotation) for any accounts that authenticated during the exposure window.
5. Step 5: Post-Incident. Document the gap between firmware patching and LDAP reconfiguration as a process control failure. Update your patch validation procedures to include multi-step remediation verification, not just firmware version confirmation. Review MFA enforcement across all remote access entry points. Reference NIST CM-6 (Configuration Settings), CIS 6.3 (Require MFA for Externally-Exposed Applications), CIS 6.4 (Require MFA for Remote Network Access), and CIS 6.5 (Require MFA for Administrative Access). Apply D3-MFA (Multi-factor Authentication) and D3-CH (Credential Hardening) as standing countermeasures.

IR / Forensic Enrichment

Triage Priority	IMMEDIATE
Escalation Criteria	Escalate to senior IR leadership and legal/compliance counsel immediately if any confirmed UPN-format MFA-bypass login is identified in the 60-day lookback, as this constitutes a confirmed access control failure on a critical remote access gateway with active exploitation confirmed between February and March 2026, triggering breach notification assessment obligations under HIPAA, PCI DSS, and applicable state privacy laws if PII or PHI was accessible from VPN-reachable network segments.
Recovery Notes	Following firmware patch and LDAP reconfiguration completion, conduct a controlled UPN-format authentication test from a non-privileged account daily for the first seven days to confirm MFA enforcement remains intact across SonicWall configuration changes or reboots. Monitor SonicWall SSL-VPN authentication logs and internal SIEM (or manual log review) for Cobalt Strike beacon patterns, lateral movement from VPN tunnel IP ranges, and new scheduled task creation for a minimum of 30 days post-remediation, consistent with the dwell time profile of initial access brokers targeting this vulnerability for ransomware staging. For Gen6 appliances approaching the April 16, 2026 EOL date, accelerate hardware replacement timelines, as post-EOL devices will not receive patches for any subsequent vulnerabilities discovered after end-of-support and represent a standing residual risk to remote access infrastructure.
Forensic Artifacts	SonicWall SSL-VPN authentication log (exported from Log > View > SSL VPN): filter for Username field containing '@' (UPN format) with null or absent MFA Challenge field — this is the primary forensic indicator that CVE-2024-12802 was exploited on a specific session, as the bypass only functions via the UPN login path | SonicWall running configuration export (System > Settings > Export Settings) captured before and after LDAP reconfiguration: the delta between these two exports documents the specific LDAP binding change that closes the UPN authentication bypass path and establishes the exact remediation timestamp for the exposure window calculation | Active Directory domain controller Windows Security Event Log, Event IDs 4768 and 4769 (Kerberos TGT and Service Ticket Requests) from the SonicWall VPN tunnel IP range during the exposure window: these reveal which internal Kerberos-authenticated resources were accessed by sessions that bypassed MFA, mapping the attacker's post-authentication lateral movement path | Windows Security Event Log Event ID 4698 (Scheduled Task Created) and Sysmon Event ID 1 (Process Creation) on hosts reachable from the VPN subnet, filtered to within 4 hours of any confirmed bypass session: initial access brokers deploying Cobalt Strike as a precursor to ransomware staging commonly establish scheduled task persistence within this window following successful VPN authentication | Network flow records or firewall session logs showing outbound connections from VPN-tunnel-assigned IPs or subsequently accessed internal hosts to external IP addresses on TCP/443, 80, or 8080 during and after suspicious VPN sessions: Cobalt Strike C2 beaconing uses these ports with malleable profiles that blend with legitimate HTTPS traffic, and the presence of periodic outbound connections at regular intervals (default 60-second beacon) to hosting infrastructure is a key indicator of post-exploitation staging consistent with the ransomware-precursor threat actor pattern described in the advisory

Per-Action IR Details

Step 1: Containment — Identify all SonicWall Gen6 SSL-VPN appliances in your environment. Restrict internet-facing VPN access to known IP ranges or place devices behind a WAF/IPS while remediation is completed. For Gen6 devices not yet at end-of-life, verify firmware has been updated to the patched version

per SonicWall's advisory. Do not assume firmware alone closes the vulnerability. Reference NIST CM-7 (Least Functionality) and CIS 4.4 (Implement and Manage a Firewall on Servers).

NIST Phase: Containment

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

Controls: NIST CM-7 (Least Functionality), NIST AC-17 (Remote Access), NIST SC-7 (Boundary Protection), CIS 4.4 (Implement and Manage a Firewall on Servers), CIS 1.1 (Establish and Maintain Detailed Enterprise Asset Inventory)

Compensating: Run a firewall rule on your perimeter device (pfSense, iptables, or Windows Firewall) to whitelist only known corporate egress IPs on TCP/443 and TCP/4433 (SonicWall SSL-VPN ports) while patching is underway. Use `nmap -p 443,4433,8443 --open` to enumerate internet-facing SonicWall management interfaces not yet inventoried. For WAF-less environments, place an nginx reverse proxy with IP allowlist in front of the VPN portal as a temporary chokepoint.

Evidence: Before restricting access, export the SonicWall SSL-VPN session log (Log > View > SSL VPN) and capture the full authentication event table showing Source IP, Username, Login Format (UPN vs. standard), and MFA Challenge Status. Archive the SonicWall firmware version string from System > Diagnostics > System Info to document pre-patch state. Preserve the LDAP authentication configuration export (System > LDAP) to confirm whether the required reconfiguration step had been applied prior to containment.

Step 2: Detection — Review SSL-VPN authentication logs for logins using UPN format (user@domain.tld) rather than standard username format, particularly from unfamiliar source IPs or VPS/VPN infrastructure ranges. Correlate against SIEM for sessions where MFA was not challenged despite MFA policy being active. Flag any successful UPN-format authentications occurring during off-hours or from geolocations inconsistent with your workforce. Reference NIST AU-6 (Audit Record Review, Analysis, and Reporting) and CIS 8.2 (Collect Audit Logs). Apply D3-LAM (Local Account Monitoring) to identify anomalous account activity post-authentication.

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), NIST SI-4 (System Monitoring), CIS 8.2 (Collect Audit Logs)

Compensating: Without a SIEM, export the SonicWall SSL-VPN authentication log as a CSV (Log > Export) and run the following PowerShell one-liner to isolate UPN-format logins: `Import-Csv sonicwall_auth.csv | Where-Object { $_.Username -match '@' } | Select-Object Timestamp, Username, SourceIP, MFAChallenged | Export-Csv upn_logins.csv -NoTypeInformation`. Cross-reference source IPs against free threat intel feeds using `curl https://api.abuseipdb.com/api/v2/check?ipAddress=` (AbuseIPDB free tier) or paste IPs into GreyNoise Community to flag VPS/hosting infrastructure. For post-authentication lateral movement detection on internal hosts, deploy Sysmon with SwiftOnSecurity's config and alert on Event ID 4624 (Logon Type 3/10) from VPN tunnel IPs to internal assets within 30 minutes of the suspicious VPN session.

Evidence: Collect the SonicWall SSL-VPN log entries for the past 60 days filtered to authentication events, specifically preserving: Username field format (presence of '@domain.tld' suffix indicates UPN-path login used by this exploit), MFA Challenge field (null or absent value on a policy-enforced account confirms bypass occurred), Source IP, Session Duration, and Bytes Transferred (large transfers post-login suggest data staging). On the downstream Active Directory domain controller, pull Windows Security Event Log for Event ID 4768 (Kerberos TGT Request) and 4769 (Kerberos Service Ticket) from the IP range assigned to SonicWall VPN tunnels, correlated to timestamps of suspicious VPN sessions, to determine what internal resources were accessed.

Step 3: Eradication — Apply the SonicWall firmware patch for CVE-2024-12802 if not already done. Then complete the required LDAP reconfiguration step documented in SonicWall's guidance to enforce MFA on the UPN login path — this step is mandatory and the firmware update alone does not remediate the vulnerability. For Gen6 devices reaching end-of-life April 16, 2026, begin hardware replacement planning immediately. Reference NIST SI-4 (System Monitoring) and CIS 7.3 (Perform Automated Operating System Patch Management).

NIST Phase: Eradication

Reference: NIST 800-61r3 §3.4 — Eradication

Controls: NIST SI-2 (Flaw Remediation), NIST CM-3 (Configuration Change Control), NIST CM-6 (Configuration Settings), CIS 7.3 (Perform Automated Operating System Patch Management), CIS 7.2 (Establish and Maintain a Remediation Process)

Compensating: For the mandatory LDAP reconfiguration step, document the exact before/after configuration state by capturing screenshots or a config export from the SonicWall management interface (System > LDAP) both before and after applying the reconfiguration, creating an auditable change record without a formal ITSM tool. For Gen6 EOL planning, use the free SonicWall Product Lifecycle page to confirm April 16, 2026 EOS date and build a one-page risk acceptance memo signed by the responsible system owner if replacement cannot occur before EOL — this creates documented acknowledgment of residual risk. Verify the LDAP reconfiguration was applied correctly by attempting a test UPN-format login from a controlled account and confirming MFA is challenged before granting access.

Evidence: Before applying the firmware patch and LDAP reconfiguration, export and preserve: the current SonicWall running configuration file (System > Settings > Export Settings) as forensic baseline; the current firmware version string; and the LDAP configuration state showing whether the UPN authentication path was previously bound to MFA enforcement. These artifacts establish the pre-remediation exposure window and are required if regulatory breach notification is triggered. After patching, capture the post-remediation configuration export and firmware version string as evidence of completed remediation for audit purposes.

Step 4: Recovery — After completing both remediation steps, validate that UPN-format authentication attempts now trigger MFA challenges. Test from a controlled account using UPN login format and confirm MFA is enforced. Review authentication logs for the prior 60 days for any successful UPN-format logins that bypassed MFA. Treat any such session as a confirmed compromise and initiate incident response. Monitor for Cobalt Strike indicators, new scheduled tasks, and unexpected driver loads. Reference NIST CP-10 (System Recovery and Reconstitution) and D3-CRO (Credential Rotation) for any accounts that authenticated during the exposure window.

NIST Phase: Recovery

Reference: NIST 800-61r3 §3.5 — Recovery

Controls: NIST CP-10 (System Recovery and Reconstitution), NIST IA-5 (Authenticator Management), NIST AC-2 (Account Management), NIST AU-6 (Audit Record Review, Analysis, and Reporting), CIS 6.3 (Require MFA for Externally-Exposed Applications), CIS 6.4 (Require MFA for Remote Network Access)

Compensating: For Cobalt Strike beacon detection without EDR, deploy the free Cobalt Strike configuration extractor (`csce` by Sentinel One, available on GitHub) against any memory dumps from hosts accessed during compromised VPN sessions. Run `schtasks /query /fo LIST /v > scheduled_tasks_baseline.txt` on all hosts reachable from the VPN subnet and diff against a known-good baseline to detect persistence via scheduled tasks — a common post-exploitation technique following initial access broker activity. Use Sysinternals Autoruns (free) to identify unexpected driver loads or registry Run key entries on endpoints that established internal connections during the suspicious VPN sessions. For credential rotation of potentially compromised accounts, use PowerShell: `Set-ADAccountPassword -Identity -Reset -NewPassword (ConvertTo-SecureString -AsPlainText '' -Force)` for each flagged UPN-format login.

Evidence: For each confirmed or suspected compromised VPN session, collect from the endpoint(s) accessed: Windows prefetch files (`C:\Windows\Prefetch\`) for evidence of attacker tooling execution; `C:\Users\\AppData\Roaming\Microsoft\Windows\Recent\` for accessed files; Windows Security Event Log Event ID 4698 (Scheduled Task Created) and 7045 (New Service Installed) within 24 hours of the VPN session; and network connection logs (Sysmon Event ID 3 or netstat snapshots) showing outbound connections to non-standard ports indicative of Cobalt Strike C2 (commonly TCP/443, 80, or 8080 to hosting infrastructure). Memory acquisition using WinPmem (free) from any host showing post-exploitation indicators should be prioritized before remediation wipes the volatile state.

Step 5: Post-Incident — Document the gap between firmware patching and LDAP reconfiguration as a process control failure. Update your patch validation procedures to include multi-step remediation verification, not

just firmware version confirmation. Review MFA enforcement across all remote access entry points. Reference NIST CM-6 (Configuration Settings), CIS 6.3 (Require MFA for Externally-Exposed Applications), CIS 6.4 (Require MFA for Remote Network Access), and CIS 6.5 (Require MFA for Administrative Access). Apply D3-MFA (Multi-factor Authentication) and D3-CH (Credential Hardening) as standing countermeasures.

NIST Phase: Post Incident

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

Controls: NIST CM-6 (Configuration Settings), NIST IR-4 (Incident Handling), NIST IA-5 (Authenticator Management), NIST PM-6 (Measures of Performance), CIS 6.3 (Require MFA for Externally-Exposed Applications), CIS 6.4 (Require MFA for Remote Network Access), CIS 6.5 (Require MFA for Administrative Access), CIS 7.1 (Establish and Maintain a Vulnerability Management Process)

Compensating: Document the firmware-only vs. firmware-plus-LDAP-reconfiguration distinction as a formal lessons-learned item and update your patch checklist template to include a 'vendor advisory secondary steps' verification field — this costs nothing and prevents recurrence of incomplete multi-step remediations. For ongoing MFA enforcement validation across remote access entry points, schedule a quarterly manual audit using the free `ldapsearch` CLI tool against your LDAP/AD instance to confirm MFA policies are bound to all VPN-authenticated user groups, not just the primary login path. Create a Sigma rule (free, YAML-based) to continuously alert on UPN-format authentication attempts against SonicWall SSL-VPN going forward, even after remediation, as a standing detection for similar authentication-path bypass techniques (MITRE T1078 — Valid Accounts).

Evidence: Compile the complete incident record including: the timeline delta between SonicWall advisory publication and LDAP reconfiguration completion (this is the organizational exposure window for regulatory purposes); a list of all user accounts that successfully authenticated via UPN format during the exposure window with corresponding session details; the pre- and post-remediation SonicWall configuration exports confirming LDAP reconfiguration state; and the results of the controlled UPN-format MFA challenge test performed in Step 4. This package constitutes the evidence record for breach notification assessment if PII or PHI was accessible from VPN-reachable systems during compromised sessions.

Detection Guidance

Primary detection focus: UPN-format authentication events in SonicWall SSL-VPN logs where MFA was not challenged. Query authentication logs for login events using the format user@domain.tld and cross-reference against your MFA enforcement policy. A successful login via UPN path with no corresponding MFA challenge event is a high-confidence indicator of bypass exploitation. Secondary indicators: source IPs resolving to VPS hosting providers (DigitalOcean, Vultr, Linode, and similar); authentication attempts from geographies inconsistent with your workforce, particularly in clusters suggesting brute-force pre-staging (T1110); successful logins followed quickly by RDP lateral movement (T1021.001) or unusual process creation events (Cobalt Strike beacon patterns, unexpected driver loads consistent with BYOVD). SIEM query logic: filter SSL-VPN auth logs for UPN-format username field AND successful authentication AND absence of MFA challenge event within the same session ID. Behavioral indicator: post-auth activity within seconds of login, suggesting scripted exploitation rather than human interaction. Reference NIST AU-3 (Content of Audit Records) to confirm your logs capture username format and MFA challenge status per session. Apply D3-SFA (System File Analysis) to review for post-exploitation persistence artifacts on systems accessed during the exposure window.

Indicators of Compromise

Type	Value	Context	Confidence
IP	`VPS/VPN infrastructure ranges (DigitalOcean, Vultr, Linode)`	Attacker infrastructure used to obscure origin during exploitation — T1090, T1583.003. Specific IPs not publicly attributed; monitor for VPN authentication from known VPS ASNs.	MEDIUM
URL	`UPN-format login path on SonicWall SSL-VPN management interface`	Authentication requests using user@domain.tld format against the UPN login path are the exploitation vector. Not a network IOC — behavioral pattern in authentication logs.	HIGH

Framework Mappings

MITRE-ATTACK

- **T1587.001** — Malware
- **T1110** — Brute Force
- **T1090** — Proxy
- **T1133** — External Remote Services
- **T1078** — Valid Accounts
- **T1486** — Data Encrypted for Impact
- **T1556** — Modify Authentication Process
- **T1078.002** — Domain Accounts
- **T1650** — Acquire Access
- **T1543** — Create or Modify System Process
- **T1583.003** — Virtual Private Server
- **T1021.001** — Remote Desktop Protocol

NIST-800-53R5

- **AC-7** — Unsuccessful Logon Attempts
- **IA-2** — Identification and Authentication (Organizational Users)
- **IA-5** — Authenticator Management
- **AC-17** — Remote Access
- **AC-20** — Use of External Systems
- **SC-7** — Boundary Protection
- **AC-2** — Account Management
- **AC-6** — Least Privilege
- **CP-9** — System Backup
- **CP-10** — System Recovery and Reconstitution
- **SI-4** — System Monitoring
- **SI-7** — Software, Firmware, and Information Integrity

- **IA-8** — Identification and Authentication (Non-Organizational Users)
- **IR-4** — Incident Handling
- **SC-13** — Cryptographic Protection
- **IR-5** — Incident Monitoring

OWASP-TOP10-2021

- **A07:2021** — Identification and Authentication Failures

CIS-V8

- **6.3** — Require MFA for Externally-Exposed Applications
- **6.4** — Require MFA for Remote Network Access
- **6.5** — Require MFA for Administrative Access
- **7.3** — Perform Automated Operating System Patch Management
- **7.4** — Perform Automated Application Patch Management
- **8.2** — Collect Audit Logs

SOC2-TSC

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

HIPAA-SECURITY

- **164.312(d)** — Person or Entity Authentication
- **164.308(a)(7)(ii)(A)** — Data Backup Plan
- **164.312(e)(1)** — Transmission Security

NIST-CSF-2

- **RS.MI-01** — Incidents are contained
- **DE.CM-01** — Networks and network services are monitored
- **DE.AE-08** — Incidents are declared when adverse events meet the defined incident criteria

ISO-27001-2022

- **A.5.29** — Information security during disruption
- **A.8.8** — Management of technical vulnerabilities

MITRE ATT&CK Mapping

Technique ID	Technique Name	Tactic
T1587.001	Malware	Resource-Development
T1110	Brute Force	Credential-Access
T1090	Proxy	Command-And-Control
T1133	External Remote Services	Persistence

Technique ID	Technique Name	Tactic
T1078	Valid Accounts	Defense-Evasion
T1486	Data Encrypted for Impact	Impact
T1556	Modify Authentication Process	Credential-Access
T1078.002	Domain Accounts	Defense-Evasion
T1650	Acquire Access	Resource-Development
T1543	Create or Modify System Process	Persistence
T1583.003	Virtual Private Server	Resource-Development
T1021.001	Remote Desktop Protocol	Lateral-Movement

Sources

Source	URL	Tier
Security News	https://www.bleepingcomputer.com/news/security/hackers-bypass-sonic...	T3
CVE-2024-12802 - NVD	https://nvd.nist.gov/vuln/detail/CVE-2024-12802	T1
CVE-2024-12802: SonicWALL SSL-VPN MFA Bypass Vulnerability	https://www.sentinelone.com/vulnerability-database/cve-2024-12802/	T3
CVE-2024-12802 - Exploits & Severity - Feedly	https://feedly.com/cve/CVE-2024-12802	T3
SSL-VPN MFA Bypass in SonicWALL SSL-VPN can arise in... - GitHub	https://github.com/advisories/GHSA-ff32-cmvq-x6c5	T3

Generated 2026-05-21 06:58 UTC by TJS Security Command Center