INTELLIGENCE BRIEFING
Security Command Center
TLP:CLEAR
2026-06-14 04:24 UTC

Velvet Ant APT: Decade-Long Persistence via Linux PAM and OpenSSH Hijacking in Air-Gapped Network

THREAT CAMPAIGN | **CRITICAL** | CVSS 9.5

SCC Item ID	SCC-CAM-2026-0453
Type	Threat Campaign
Severity	CRITICAL
CVSS Base Score	9.5
Affected Products	Linux PAM (pam_unix.so), OpenSSH (ssh, sshd, scp), Nginx, fcgiwrap, F5 BIG-IP (prior campaign), Cisco NX-OS/Nexus switches (prior campaign)
Published	2026-06-13T10:06:42
Discovery Source	Rss

Executive Summary

A Chinese state-sponsored threat group known as Velvet Ant maintained covert access inside a large organization's air-gapped critical infrastructure network for approximately ten years, beginning in 2016, without detection. The attackers compromised core Linux authentication libraries and OpenSSH binaries, enabling persistent credential harvesting and remote access that survived routine security reviews and was extremely difficult to eradicate without disrupting live operations. Organizations running Linux-based critical infrastructure, particularly those with legacy air-gapped segments or network appliances from F5 and Cisco, face elevated risk from this tradecraft.

Technical Analysis

Velvet Ant (China-nexus APT) executed a multi-stage intrusion documented by Sygnia as Operation Highland. Initial access leveraged internet-facing infrastructure, with prior-campaign footholds established via F5 BIG-IP appliances and Cisco NX-OS/Nexus switches. Pivot into the air-gapped segment was achieved using Nginx and FastCGI (fcgiwrap) as an execution bridge. Deep persistence was established by hijacking two Linux authentication components: pam_unix.so (Linux PAM) and OpenSSH binaries (ssh, sshd, scp). Malicious code embedded directly into the authentication stack intercepted all authentication events and harvested credentials in plaintext. Relevant CWEs: CWE-312 (Cleartext Storage of Sensitive Information), CWE-506 (Embedded Malicious Code), CWE-494 (Download of Code Without Integrity Check), CWE-287 (Improper Authentication). No single CVE ID is assigned to the campaign; the intrusion exploited configuration weaknesses and

supply-chain-level binary tampering rather than a discrete patched vulnerability. MITRE ATT&CK techniques include T1556.003 (Pluggable Authentication Modules), T1601.001 (Patch System Image), T1543.002 (Systemd Service), T1090.001 (Internal Proxy), T1505.003 (Web Shell), T1021.004 (SSH), T1573 (Encrypted Channel), and T1070 (Indicator Removal). A related F5 BIG-IP SCP/SFTP vulnerability (CVE-2025-53868) is referenced in the source set and should be reviewed in the context of this actor's targeting of F5 appliances.

Action Checklist

1. Step 1: Containment. Isolate any Linux hosts in air-gapped or semi-isolated segments that share authentication infrastructure with internet-facing systems. Specifically audit Nginx and fcgiwrap deployments acting as execution bridges between network segments. Block lateral SSH movement from edge appliances (F5 BIG-IP, Cisco Nexus) into internal Linux hosts pending integrity verification. Apply CIS 4.4 (Implement and Manage a Firewall on Servers) to restrict SSH access to explicitly authorized management hosts only.
2. Step 2: Detection. Compare cryptographic hashes of pam_unix.so and all OpenSSH binaries (ssh, sshd, scp) against known-good hashes from the distribution vendor's signed package repository. Query file integrity monitoring logs for unexpected modification timestamps on /lib/security/pam_unix.so, /usr/sbin/sshd, /usr/bin/ssh, and /usr/bin/scp. Review auth.log and syslog for authentication events that do not produce corresponding PAM debug entries, which may indicate intercepted authentication. Audit Nginx access logs for anomalous FastCGI invocations, particularly requests to fcgiwrap endpoints not associated with normal application traffic. Map observed activity to NIST AU-6 (Audit Record Review, Analysis, and Reporting) and AU-12 (Audit Record Generation) to verify logging coverage across affected hosts.
3. Step 3: Eradication. Reinstall Linux PAM and OpenSSH packages from verified, cryptographically signed distribution sources on all affected or suspect hosts; do not patch in place over potentially compromised binaries. Rebuild hosts from trusted images where feasible, consistent with NIST CM controls. Rotate all credentials (passwords, SSH keys, certificates) that were authenticated through any potentially compromised PAM or SSH stack, per D3-CRO (Credential Rotation). Remove or disable Nginx/fcgiwrap execution bridges that served as the cross-segment pivot path. Review and remediate CVE-2025-53868 on F5 BIG-IP appliances per the F5 advisory at https://my.f5.com/manage/s/article/K000151902 (validate URL against F5 official support portal before use).
4. Step 4: Recovery. After reinstallation, re-hash all authentication binaries and record baseline hashes in a file integrity monitoring system under NIST SI-4 (System Monitoring) controls. Validate that no residual web shells or FastCGI backdoors remain on Nginx hosts. Confirm SSH key inventories are complete and all pre-rotation keys are revoked. Monitor authentication logs for 30 days post-remediation for signs of re-entry, paying particular attention to off-hours authentication attempts and source IPs inconsistent with authorized management infrastructure. Apply CIS 8.2 (Collect Audit Logs) to ensure centralized, tamper-resistant log collection is active across all remediated hosts.
5. Step 5: Post-Incident. This intrusion exposed gaps in binary integrity monitoring for OS-level authentication components and insufficient network segmentation enforcement between edge appliances and air-gapped segments. Implement continuous file integrity monitoring (D3-SFA, System File Analysis) covering PAM modules and SSH binaries as a standing control. Enforce MFA for all administrative and remote access paths per CIS 6.4 (Require MFA for Remote Network Access) and CIS 6.5 (Require MFA for Administrative Access) and D3-MFA. Establish a formal supply-chain integrity verification process for OS package installations (CWE-494 remediation). Review and update network segmentation architecture

to eliminate FastCGI or equivalent execution-bridge patterns crossing trust boundaries.

IR / Forensic Enrichment

Triage Priority	IMMEDIATE
Escalation Criteria	Escalate immediately to senior leadership, legal counsel, and (where applicable) regulatory bodies if any evidence confirms that Velvet Ant's credential-harvesting implant captured authentication material for privileged accounts accessing classified, OT/ICS, PII, or PHI systems, or if any air-gapped segment containing critical infrastructure control systems shows indicators of the PAM or SSH binary tampering described in this campaign.
Recovery Notes	Before returning any remediated host to production, independently verify that the reinstalled pam_unix.so and all OpenSSH binaries hash identically to the distribution vendor's published checksums — do not rely solely on the package manager's internal database, which Velvet Ant may have modified to conceal tampering. Monitor all remediated hosts for a minimum of 30 days post-eradication, focusing on off-hours SSH authentications, any new fcgiwrap or FastCGI process spawning, and any file modification events under /lib/security/ or /usr/sbin/ that occur outside of an authorized change window. Given Velvet Ant's demonstrated decade-long persistence and ability to survive routine security reviews, treat re-detection of PAM or SSH anomalies within 90 days as evidence of incomplete eradication rather than a new incident, and initiate full reimaging of the affected host.
Forensic Artifacts	Hijacked pam_unix.so and sshd binaries: SHA-256 hashes of /lib/security/pam_unix.so, /usr/sbin/sshd, /usr/bin/ssh, and /usr/bin/scp compared against the distribution vendor's signed package checksums — hash mismatches are the primary indicator of Velvet Ant binary-level tampering and must be preserved as evidence before eradication. | Credential harvest output files: Search for hidden or world-writable files in /tmp, /dev/shm, /var/tmp, and dot-directories under root and service account home directories for files containing SSH credential patterns — Velvet Ant's pam_unix.so implant logged captured credentials to local files before exfiltration. | Nginx and fcgiwrap access logs: /var/log/nginx/access.log entries showing POST requests or unusual GET parameters to fcgiwrap endpoints, particularly requests originating from F5 BIG-IP or Cisco Nexus management IP ranges, which document the cross-segment execution bridge Velvet Ant used to reach air-gapped hosts. | SSH daemon memory dump: A RAM acquisition (LiME) focused on the sshd process address space, which will contain plaintext credentials captured by the PAM hook before they were written to disk — this is the highest-value volatile artifact and is destroyed the moment sshd is killed or the host is isolated. | Package manager modification logs: /var/log/dpkg.log (Debian) or /var/log/rpm/history.log (RPM) covering the full suspected intrusion window from 2016 onward, cross-referenced against authorized change records — gaps, backdated entries, or reinstall events with no corresponding change ticket are indicators that Velvet Ant used legitimate package tooling to install their trojanized binaries.

Per-Action IR Details

Step 1: Containment — Isolate any Linux hosts in air-gapped or semi-isolated segments that share authentication infrastructure with internet-facing systems. Specifically audit Nginx and fcgiwrap deployments acting as execution bridges between network segments. Block lateral SSH movement from edge appliances (F5 BIG-IP, Cisco Nexus) into internal Linux hosts pending integrity verification. Apply CIS 4.4 (Implement and Manage a Firewall on Servers) to restrict SSH access to explicitly authorized management hosts only.

NIST Phase: Containment

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

Controls: CIS 4.4 (IG1/IG2/IG3) — Implement and Manage a Firewall on Servers, NIST AC-4 — Information Flow Enforcement, NIST AC-17 — Remote Access

Compensating: On each Linux host, deploy an iptables allowlist immediately: `iptables -A INPUT -p tcp --dport 22 -s -j ACCEPT && iptables -A INPUT -p tcp --dport 22 -j DROP`. On Cisco Nexus switches, apply a vty ACL restricting SSH source to the management VLAN: `ip access-list SSH-MGMT / permit tcp any eq 22 / deny tcp any any eq 22`. Enumerate fcgiwrap socket listeners with `ss -xlp | grep fcgi` and disable non-essential instances via systemctl. Document all rules before applying so rollback is one command.

Evidence: Before isolating any host, capture live network state to preserve evidence of active Velvet Ant SSH tunnels and fcgiwrap-mediated connections that will be severed on isolation: run `ss -tnp` and `netstat -ano` to record all established TCP connections and associated PIDs; capture `ip route` and ARP table (`arp -n`) to document cross-segment routing; collect `lsof -i -n -P` output to map open file descriptors to SSH/Nginx processes. Dump `/proc//maps` and `/proc//maps` to identify any memory-mapped shared objects that may reflect the hijacked pam_unix.so or patched sshd binary. Snapshot these before any firewall rule change, as established sessions will drop immediately on isolation.

Step 2: Detection — Compare cryptographic hashes of pam_unix.so and all OpenSSH binaries (ssh, sshd, scp) against known-good hashes from the distribution vendor's signed package repository. Query file integrity monitoring logs for unexpected modification timestamps on /lib/security/pam_unix.so, /usr/sbin/sshd, /usr/bin/ssh, and /usr/bin/scp. Review auth.log and syslog for authentication events that do not produce corresponding PAM debug entries, which may indicate intercepted authentication. Audit Nginx access logs for anomalous FastCGI invocations, particularly requests to fcgiwrap endpoints not associated with normal application traffic. Map observed activity to NIST AU-6 (Audit Record Review, Analysis, and Reporting) and AU-12 (Audit Record Generation) to verify logging coverage across affected hosts.

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-12 — Audit Record Generation, NIST AU-3 — Content Of Audit Records, CIS 8.2 (IG1/IG2/IG3) — Collect Audit Logs

Compensating: Use `rpm -V openssh pam` (RPM-based) or `debsums -c libpam-modules openssh-server openssh-client` (Debian-based) to detect binary drift against the package manager's recorded checksums — note this will miss tampering if the package database itself was altered, so also independently compute SHA-256 hashes: `sha256sum /lib/security/pam_unix.so /usr/sbin/sshd /usr/bin/ssh /usr/bin/scp` and compare against the vendor's published checksums. Deploy osquery with the FIM pack to query `SELECT * FROM file WHERE path IN ('/lib/security/pam_unix.so','/usr/sbin/sshd') AND mtime > ;`. Write a Sigma rule targeting auth.log for successful authentication events (`sshd: Accepted`) with no preceding `pam_unix(sshd:auth)` entry in the same session window. Grep Nginx access logs for fcgiwrap invocations: `grep -E 'fcgi|cgi-bin' /var/log/nginx/access.log | awk '{print $1,$7,$9}' | sort | uniq -c | sort -rn`.

Evidence: This step alters no live state; however, collect volatile artifacts concurrently before any subsequent containment action invalidates them. Specifically: capture `/proc//exe` symlink resolution and `md5sum /proc//exe` — a hijacked sshd will show a hash mismatch against the on-disk binary if the binary was replaced after process start; capture `strings /proc//mem` fragments (via gcore or manual mapping) to identify credential-harvesting strings embedded in the hijacked pam_unix.so at runtime; pull `/var/log/auth.log` and `/var/log/syslog` covering the entire suspected compromise window (2016 onward if available); export Nginx `access.log` and `error.log` from all hosts running fcgiwrap; record `/etc/pam.d/sshd` and `/etc/pam.d/common-auth` contents to detect Velvet Ant PAM stack modifications; document all currently loaded PAM modules via `pam-auth-update --list` or equivalent.

Step 3: Eradication — Reinstall Linux PAM and OpenSSH packages from verified, cryptographically signed distribution sources on all affected or suspect hosts; do not patch in place over potentially compromised binaries. Rebuild hosts from trusted images where feasible, consistent with NIST CM controls. Rotate all credentials (passwords, SSH keys, certificates) that were authenticated through any potentially compromised PAM or SSH stack, per D3-CRO (Credential Rotation). Remove or disable Nginx/fcgiwrap execution bridges

that served as the cross-segment pivot path. Review and remediate CVE-2025-53868 on F5 BIG-IP appliances per the F5 advisory at https://my.f5.com/manage/s/article/K000151902 (search-retrieved URL — validate before use).

NIST Phase: Eradication

Reference: NIST 800-61r3 §3.4 — Eradication

Controls: NIST AC-2 — Account Management, NIST AC-3 — Access Enforcement, CIS 7.3 (IG1/IG2/IG3) — Perform Automated Operating System Patch Management, CIS 7.4 (IG1/IG2/IG3) — Perform Automated Application Patch Management, CIS 5.1 (IG1/IG2/IG3) — Establish and Maintain an Inventory of Accounts

Compensating: Before reinstalling, take a full disk image of the compromised host for forensic preservation: `dd if=/dev/sda bs=4M | gzip > /forensics/hostname_$(date +%Y%m%d).img.gz`. Reinstall PAM and OpenSSH in a verified state: `apt-get install --reinstall libpam-modules openssh-server openssh-client` (verify GPG signature on package download). For SSH key rotation, use `find /root /home -name 'authorized_keys' -exec cat {} \;` to inventory all trusted keys, then deprovision all pre-incident keys and issue new ED25519 key pairs: `ssh-keygen -t ed25519 -C 'rotated-$(date +%Y%m%d)'`. Disable fcgiwrap: `systemctl stop fcgiwrap && systemctl disable fcgiwrap && systemctl mask fcgiwrap`. For hosts where full rebuild is not feasible, use `LD_PRELOAD=` checks and `ldd /usr/sbin/sshd` to confirm no injected shared library paths remain.

Evidence: This step permanently alters live state — full forensic preservation MUST precede reinstallation. Before any package reinstall or credential rotation: acquire a full RAM dump using LiME (`insmod lime.ko path=/forensics/mem.lime format=lime`) to capture plaintext credentials that Velvet Ant's harvesting implant stored in sshd process memory; preserve `/etc/shadow`, `/etc/passwd`, `/etc/ssh/sshd_config`, and all `/etc/pam.d/` files; collect all files with modification timestamps within the suspected intrusion window using `find / -newer /var/log/dpkg.log -type f -ls 2>/dev/null > /forensics/modified_files.txt`; record running process tree (`ps auxf`) and loaded kernel modules (`lsmod`) before any process termination; hash all four target binaries one final time immediately before reinstall as the authenticated pre-eradication state record.

Step 4: Recovery — After reinstallation, re-hash all authentication binaries and record baseline hashes in a file integrity monitoring system under NIST SI-4 (System Monitoring) controls. Validate that no residual web shells or FastCGI backdoors remain on Nginx hosts. Confirm SSH key inventories are complete and all pre-rotation keys are revoked. Monitor authentication logs for 30 days post-remediation for signs of re-entry, paying particular attention to off-hours authentication attempts and source IPs inconsistent with authorized management infrastructure. Apply CIS 8.2 (Collect Audit Logs) to ensure centralized, tamper-resistant log collection is active across all remediated hosts.

NIST Phase: Recovery

Reference: NIST 800-61r3 §3.5 — Recovery

Controls: NIST AU-9 — Protection Of Audit Information, NIST AU-11 — Audit Record Retention, NIST AU-8 — Time Stamps, CIS 8.2 (IG1/IG2/IG3) — Collect Audit Logs, CIS 5.3 (IG1/IG2/IG3) — Disable Dormant Accounts

Compensating: Immediately post-reinstall, record authoritative baseline hashes: `sha256sum /lib/security/pam_unix.so /usr/sbin/sshd /usr/bin/ssh /usr/bin/scp /usr/bin/scp > /etc/security/binary_baseline_$(date +%Y%m%d).sha256` — store this file on a read-only or out-of-band system so Velvet Ant cannot overwrite it. Scan Nginx document root and CGI directories for web shells using ClamAV: `clamscan -r /var/www /usr/lib/cgi-bin --infected --remove=no`. Set up a daily cron job to re-verify binary hashes against the baseline and alert on mismatch: `0 3 * * * sha256sum -c /etc/security/binary_baseline.sha256 | mail -s 'PAM/SSH integrity check' soc@example.com`. Forward auth.log to a centralized syslog server using rsyslog `@@remote-syslog:514` to ensure logs cannot be altered locally by a re-established implant.

Evidence: Before returning hosts to production, verify eradication was complete: re-run `debsums -c libpam-modules openssh-server` on the freshly installed system and confirm zero mismatches; check `/proc/1/maps` and `lsof` on the new sshd process to confirm pam_unix.so is loaded from the expected distribution path with no alternate shared library injections; confirm no residual cron entries (`crontab -l -u root`), systemd unit files (`systemctl list-units --all | grep -i fcgi`), or SUID binaries (`find / -perm -4000 -ls`) were left behind by the threat actor. Verify NTP synchronization on all remediated hosts (`timedatectl status`) to ensure post-recovery auth.log timestamps are trustworthy for the 30-day

watch period.

Step 5: Post-Incident — This intrusion exposed gaps in binary integrity monitoring for OS-level authentication components and insufficient network segmentation enforcement between edge appliances and air-gapped segments. Implement continuous file integrity monitoring (D3-SFA, System File Analysis) covering PAM modules and SSH binaries as a standing control. Enforce MFA for all administrative and remote access paths per CIS 6.4 (Require MFA for Remote Network Access) and CIS 6.5 (Require MFA for Administrative Access) and D3-MFA. Establish a formal supply-chain integrity verification process for OS package installations (CWE-494 remediation). Review and update network segmentation architecture to eliminate FastCGI or equivalent execution-bridge patterns crossing trust boundaries.

NIST Phase: Post Incident

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

Controls: CIS 6.3 (IG1/IG2/IG3) — Require MFA for Externally-Exposed Applications, CIS 6.4 (IG1/IG2/IG3) — Require MFA for Remote Network Access, CIS 6.5 (IG1/IG2/IG3) — Require MFA for Administrative Access, CIS 4.2 (IG1/IG2/IG3) — Establish and Maintain a Secure Configuration Process for Network Infrastructure, NIST AU-2 — Event Logging, NIST AU-12 — Audit Record Generation

Compensating: Implement AIDE (Advanced Intrusion Detection Environment) as a free FIM solution: `aide --init` to create baseline database post-rebuild, then schedule daily checks with `aide --check` and alert on any modification to `/lib/security/`, `/usr/sbin/sshd`, and `/usr/bin/ssh*`. For MFA on SSH without enterprise tooling, deploy Google Authenticator PAM module (`libpam-google-authenticator`) and configure `/etc/pam.d/sshd` to require TOTP alongside key-based auth — this directly addresses Velvet Ant's PAM hijacking vector by adding an authentication factor that the harvesting implant cannot replay. Write a Sigma rule for auth.log to flag authentication from source IPs outside the approved management CIDR: `sshd Accepted .* from (?!)`. Document a formal OS package integrity checklist requiring GPG verification (`apt-key list`, `rpm --checksig`) before any PAM or SSH package installation.

Evidence: The primary post-incident deliverable for this threat is a formal lessons-learned report documenting: (1) the earliest provable evidence of pam_unix.so or sshd binary modification, derived from filesystem metadata, package manager logs (`/var/log/dpkg.log`, `/var/log/rpm/history.log`), and any FIM baseline snapshots predating the compromise; (2) a complete timeline of Velvet Ant lateral movement from F5/Nexus edge appliances through the Nginx/fcgiwrap bridge into air-gapped hosts, reconstructed from Nginx access logs, auth.log, and network flow records; (3) an inventory of every credential (password hash, SSH authorized key) that transited the compromised PAM/SSH stack and therefore must be treated as permanently compromised regardless of the rotation performed during eradication.

Detection Guidance

Primary detection focus is binary integrity verification of the Linux authentication stack. Use package manager verification commands (e.g., rpm -V openssh pam or dpkg --verify openssh-server libpam-modules) to identify files with modified checksums. Cross-reference against vendor-signed package hashes. File integrity monitoring (aligned with D3-SFA) should baseline and continuously monitor /lib/security/pam_unix.so, /usr/sbin/sshd, /usr/bin/ssh, and /usr/bin/scp. Behavioral indicators include: authentication events in auth.log that bypass expected PAM module chains; sshd processes spawning unexpected child processes or making outbound network connections; Nginx access logs showing POST requests to fcgiwrap endpoints with non-standard URI patterns or payloads. Hunt for T1556.003 (PAM hijacking) by auditing PAM configuration files (/etc/pam.d/) for unauthorized module entries and verifying pam_unix.so inode/mtime against package manager records. For T1601.001 (Patch System Image), check kernel and core binary modification timestamps against last authorized maintenance windows. Collect and centralize auth.log, syslog, and Nginx access logs per NIST AU-2 and AU-12 to support retrospective analysis. Credential harvesting activity may surface as unusual authentication patterns from previously unseen source IPs using valid credentials shortly after logon to a potentially compromised host.

Indicators of Compromise

Type	Value	Context	Confidence
HASH	`not-provided-in-source-material`	Specific file hashes for trojanized pam_unix.so and OpenSSH binaries were not included in the provided source data. Refer to Sygnia's Operation Highland report at https://www.sygnia.co/blog/operation-highland-velvet-ant/ for IOC details (search-retrieved URL — validate before use).	LOW
URL	`not-provided-in-source-material`	C2 URLs or callback domains associated with this campaign were not included in the provided source data. Consult the Sygnia and Microsoft source reports for network-based IOCs.	LOW

Framework Mappings

MITRE-ATTACK

- **T1078** — Valid Accounts
- **T1543** — Create or Modify System Process
- **T1090** — Proxy
- **T1543.002** — Systemd Service
- **T1556.003** — Pluggable Authentication Modules
- **T1027** — Obfuscated Files or Information
- **T1036.005** — Match Legitimate Resource Name or Location
- **T1070** — Indicator Removal
- **T1556.004** — Network Device Authentication
- **T1190** — Exploit Public-Facing Application
- **T1552.004** — Private Keys
- **T1556** — Modify Authentication Process
- **T1601** — Modify System Image
- **T1090.001** — Internal Proxy
- **T1505.003** — Web Shell
- **T1071.001** — Web Protocols
- **T1055** — Process Injection
- **T1601.001** — Patch System Image
- **T1021.004** — SSH
- **T1573** — Encrypted Channel

NIST-800-53R5

- **AC-2** — Account Management
- **AC-6** — Least Privilege
- **IA-2** — Identification and Authentication (Organizational Users)
- **IA-5** — Authenticator Management
- **SI-3** — Malicious Code Protection
- **SI-4** — System Monitoring
- **CA-8** — Penetration Testing
- **RA-5** — Vulnerability Monitoring and Scanning
- **SC-7** — Boundary Protection
- **SI-2** — Flaw Remediation
- **SI-7** — Software, Firmware, and Information Integrity
- **CM-2** — Baseline Configuration
- **CM-7** — Least Functionality
- **CM-3** — Configuration Change Control
- **IA-8** — Identification and Authentication (Non-Organizational Users)

OWASP-TOP10-2021

- **A08:2021** — Software and Data Integrity Failures
- **A07:2021** — Identification and Authentication Failures

CIS-V8

- **2.5** — Allowlist Authorized Software
- **2.6** — Allowlist Authorized Libraries
- **6.3** — Require MFA for Externally-Exposed Applications
- **6.4** — Require MFA for Remote Network Access
- **6.5** — Require MFA for Administrative Access
- **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

NIST-CSF-2

- **DE.CM-01** — Networks and network services are monitored

MITRE ATT&CK Mapping

Technique ID	Technique Name	Tactic
T1078	Valid Accounts	Defense-Evasion
T1543	Create or Modify System Process	Persistence
T1090	Proxy	Command-And-Control
T1543.002	Systemd Service	Persistence
T1556.003	Pluggable Authentication Modules	Credential-Access
T1027	Obfuscated Files or Information	Defense-Evasion
T1036.005	Match Legitimate Resource Name or Location	Defense-Evasion
T1070	Indicator Removal	Defense-Evasion
T1556.004	Network Device Authentication	Credential-Access
T1190	Exploit Public-Facing Application	Initial-Access
T1552.004	Private Keys	Credential-Access
T1556	Modify Authentication Process	Credential-Access
T1601	Modify System Image	Defense-Evasion
T1090.001	Internal Proxy	Command-And-Control
T1505.003	Web Shell	Persistence
T1071.001	Web Protocols	Command-And-Control
T1055	Process Injection	Defense-Evasion
T1601.001	Patch System Image	Defense-Evasion
T1021.004	SSH	Lateral-Movement
T1573	Encrypted Channel	Command-And-Control

Sources

Source	URL	Tier
Security News	https://www.bleepingcomputer.com/news/security/chinese-hackers-hija...	T3
Velvet Ant's Operation Highland: How a China-Nexus Actor ... - Sygnia	https://www.sygnia.co/blog/operation-highland-velvet-ant/	T3

Source	URL	Tier
K000151902: BIG-IP SCP and SFTP vulnerability CVE-2025-53868	https://my.f5.com/manage/s/article/K000151902	T3
Multi-stage Linux intrusion via F5 and Confluence - Microsoft	https://www.microsoft.com/en-us/security/blog/2026/05/22/from-edge-...	T1
Cisco NX-OS Software CLI Command Injection Vulnerability	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecuri...	T3

Generated 2026-06-14 04:24 UTC by TJS Security Command Center