INTELLIGENCE BRIEFING
Security Command Center
TLP:CLEAR
2026-05-23 06:27 UTC

EOL F5 BIG-IP Exploitation Enables Multi-Stage Pivot to Active Directory via Confluence Credential Theft and Kerberos Relay

THREAT CAMPAIGN | **CRITICAL** | CVSS 9.5

SCC Item ID	SCC-CAM-2026-0354
Type	Threat Campaign
CVE ID	CVE-2025-33073
Severity	CRITICAL
CVSS Base Score	9.5
EPSS Score	0.2964 (97th percentile)
Affected Products	F5 BIG-IP v15.1.201000 (EOL December 31, 2024), Atlassian Confluence (unpatched), Microsoft Active Directory, Azure-hosted infrastructure
Published	2026-05-22T16:53:39+00:00
Discovery Source	Rss:T1 Threatintel

Executive Summary

An unattributed threat actor exploited an end-of-life F5 BIG-IP appliance to gain an initial foothold, then chained credential theft from an unpatched Atlassian Confluence server into Kerberos relay attacks against Active Directory and Azure-hosted infrastructure via CVE-2025-33073 (CVSS 9.5). The attack succeeded through accumulated security debt: expired perimeter appliances, over-privileged service accounts, and embedded credentials in Confluence, not novel zero-day techniques. Organizations running EOL network edge devices alongside unpatched internal collaboration platforms face immediate risk of full Active Directory compromise and cloud tenant access loss.

Technical Analysis

The attack chain begins at an EOL F5 BIG-IP v15.1.201000 (EOL: December 31, 2024) exposed at the network perimeter. The threat actor obtained SSH access to an internal Linux host via the EOL appliance, then pivoted laterally to an unpatched Atlassian Confluence server (version unspecified) to harvest embedded credentials stored in Confluence pages or configuration files (T1552.001, CWE-522). Those credentials were used to execute a Kerberos relay attack against Active Directory via CVE-2025-33073 (CVSS 9.5, EPSS 0.296 / 96.7th percentile), leveraging LLMNR/NBT-NS poisoning or similar relay technique (T1557.001, T1558.003). The actor

subsequently accessed Azure-hosted infrastructure, indicating successful cloud credential theft or token abuse (T1550). The CWE profile spans the full chain: CWE-502 (deserialization on the F5 or Confluence vector), CWE-287 (improper authentication at the perimeter), CWE-522 (unprotected credentials in Confluence), CWE-269 (over-privileged service accounts enabling escalation), and CWE-863 (authorization bypass in AD relay). Per Microsoft's analysis of SolarWinds Web Help Desk exploitation, the pattern mirrors this campaign: internet-exposed or EOL edge appliances as initial access (T1190), followed by internal application credential harvesting as the escalation path. No patch from F5 is available for EOL hardware; CVE-2025-33073 carries an MSRC advisory. CISA KEV listing has not been confirmed as of the configuration date.

Action Checklist

1. Step 1: Containment. Immediately isolate any F5 BIG-IP appliance running v15.1.x (EOL December 31, 2024) from internet-facing exposure; place on a separate, isolated management network or take offline. Block SSH (port 22) inbound to internal Linux hosts from perimeter appliance segments at the firewall layer. Enforce network segmentation between Confluence servers and Active Directory domain controllers per NIST SC-7 (Boundary Protection) and CIS 4.4.
2. Step 2: Detection. Query SIEM for SSH lateral movement from perimeter appliance IP ranges to internal Linux hosts (T1021.004). Search Confluence access logs for bulk page reads or API calls exporting content at unusual hours (T1552.001). Hunt for Kerberos AS-REP Roasting or relay events in AD Security event logs: Event ID 4768 (Kerberos TGT requests) with RC4 encryption type 0x17 from non-standard hosts, and Event ID 4769 (service ticket requests) from unexpected source IPs (T1558.003). Check Azure AD sign-in logs for authentications from on-premises service account UPNs originating from unexpected IPs or user agents (T1550). Review for new scheduled tasks (Event ID 4698, T1053.005) and new accounts created post-initial-access (T1136). Apply D3-LAM (Local Account Monitoring) and D3-SFA (System File Analysis) on affected Linux hosts.
3. Step 3: Eradication. Replace EOL F5 BIG-IP v15.1.x with a supported version (F5 BIG-IP 17.x or later) or an equivalent supported appliance; no security patch exists for EOL hardware. Apply the MSRC patch for CVE-2025-33073 per the Microsoft Security Advisory (https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-33073). Apply all outstanding Confluence security patches per Atlassian's current advisory stream. Rotate all service account credentials identified in Confluence pages or configuration exports (D3-CRO, NIST IA-5). Remove embedded credentials from Confluence entirely; enforce secrets management tooling. Reset krbtgt account password twice in AD to invalidate any forged Kerberos tickets (T1558).
4. Step 4: Recovery. Validate no persistence mechanisms remain: audit scheduled tasks (T1053.005), startup config entries (T1547.005), and DLL search-order hijacking artifacts (T1574.001) on affected Linux and Windows hosts per D3-SICA. Confirm Confluence is running a patched, supported version before reconnecting to internal networks. Verify Azure AD Conditional Access policies block legacy authentication and enforce MFA on all service accounts (CIS 6.3, CIS 6.5, D3-MFA). Re-audit AD for unauthorized accounts or group membership changes created during the intrusion window (NIST AC-2). Monitor for re-exploitation attempts against the replacement perimeter appliance for 30 days post-remediation using enhanced logging per NIST AU-6.
5. Step 5: Post-Incident. Formalize an EOL asset decommission policy with tracked sunset dates for all perimeter appliances (CIS 2.2, NIST CM-8). Implement a secrets scanning process for Confluence and internal wikis to detect embedded credentials before attackers find them (CWE-522 remediation, NIST IA-5(7)). Enforce least-privilege on all service accounts used by Confluence and adjacent internal

applications (NIST AC-6, CIS 5.4). Deploy LLMNR/NBT-NS disable policy via Group Policy to eliminate the Kerberos relay attack surface (T1557.001 mitigation). Conduct a full asset inventory review against EOL schedules quarterly (CIS 1.1, CIS 7.1).

IR / Forensic Enrichment

Triage Priority	IMMEDIATE
Escalation Criteria	Escalate to senior IR leadership, legal counsel, and executive stakeholders immediately if: (1) the Kerberos relay resulted in a Domain Admin or krbtgt compromise confirmed via Event ID 4769 with elevated ticket flags, (2) Azure AD sign-in logs confirm successful authentication from attacker-controlled IPs using on-premises service account UPNs, or (3) Confluence page exports confirm that credentials for regulated data systems (PII, PHI, PCI-scoped) were accessible — any of these conditions may trigger state breach notification obligations or SEC cybersecurity incident disclosure requirements under 17 CFR 229.106.
Recovery Notes	Before reconnecting any affected system to production networks, verify the krbtgt double-reset has fully replicated to all DCs using `repadmin /showrepl` and confirm zero legacy authentication events for Confluence service account UPNs in Azure AD for a minimum 72-hour clean window. Monitor the replacement F5 BIG-IP 17.x management interface and all internal Linux hosts that received SSH connections from the BIG-IP IP range for at least 30 days using enhanced logging (Sysmon EventID 1, 3, 11 on Windows; auditd syscall logging on Linux) to detect any re-entry through overlooked persistence. Treat any new RC4 Kerberos ticket request (Event ID 4768 etype 0x17) from the Confluence server IP during the monitoring window as a confirmed re-compromise indicator requiring immediate re-containment.
Forensic Artifacts	F5 BIG-IP TMOS qkview bundle (`/var/log/ltm`, `/var/log/audit`, `/var/log/secure`, `/var/log/tmm`, `/config/bigip.conf`) — preserves attacker-modified iRules, iCall scripts, and any TMOS persistence mechanisms injected post-initial-access on the EOL v15.1.x appliance | Confluence `confluence-access.log` REST API call sequences — bulk sequential requests to `/rest/api/content` endpoints from a single source IP during off-hours are the primary forensic indicator of T1552.001 credential harvesting from Confluence page content | Active Directory Security Event Log exports from all DCs scoped to Event IDs 4768 (TGT request with etype 0x17 RC4), 4769 (service ticket request from Confluence IP), 4720 (new account creation), and 4728/4732/4756 (privileged group membership changes) covering the full suspected intrusion window | Azure AD sign-in logs for all on-premises service account UPNs synchronized to Entra ID — attacker reuse of Confluence service account credentials for Azure authentication leaves user agent strings consistent with Impacket or PowerShell remoting rather than browser-based SSO flows | Linux `/var/log/auth.log` and `/root/.ssh/authorized_keys` plus `/home/*/.ssh/authorized_keys` on all internal Linux hosts that accepted SSH connections from the BIG-IP management IP range — SSH lateral movement via T1021.004 from a compromised perimeter appliance characteristically deposits attacker public keys for persistent re-entry

Per-Action IR Details

Step 1: Containment — Immediately isolate any F5 BIG-IP appliance running v15.1.x (EOL December 31, 2024) from internet-facing exposure; place behind out-of-band management network or take offline. Block SSH (port 22) inbound to internal Linux hosts from perimeter appliance segments at the firewall layer. Enforce network segmentation between Confluence servers and Active Directory domain controllers per NIST SC-7 (Boundary Protection) and CIS 4.4.

NIST Phase: Containment

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

Controls: NIST SC-7 (Boundary Protection), NIST IR-4 (Incident Handling), CIS 4.4 (Implement and Manage a Firewall on Servers), CIS 4.5 (Implement and Manage a Firewall on End-User Devices)

Compensating: On the upstream router or firewall, apply an ACL rule blocking TCP/22 from the F5 BIG-IP management VLAN to all internal RFC1918 ranges immediately: `iptables -I FORWARD -s -p tcp --dport 22 -j DROP`. For Confluence-to-DC isolation, add a Windows Firewall rule on DCs via GPO: `New-NetFirewallRule -DisplayName 'Block Confluence to DC' -Direction Inbound -RemoteAddress -Action Block`. Verify with `netstat -an` on DCs to confirm no established sessions from Confluence IP exist before applying.

Evidence: Before isolating the BIG-IP appliance, capture a full memory image of the running TMOS process using F5's `qkview` diagnostic bundle (`tmsh run util qkview`) — this preserves in-memory configuration, active session tables, and any injected iRules or iCall scripts that may represent attacker persistence. Export `/var/log/ltm`, `/var/log/audit`, `/var/log/secure`, and `/var/log/tmm` from the BIG-IP filesystem. On Confluence hosts, snapshot current network connections with `ss -tulpan > connections_$(date +%F_%T).txt` and capture running process list with `ps auxf` before any isolation action disrupts attacker staging. Document all current SSH established sessions on internal Linux hosts via `who -a` and `last -n 50`.

Step 2: Detection — Query SIEM for SSH lateral movement from perimeter appliance IP ranges to internal Linux hosts (T1021.004). Search Confluence access logs for bulk page reads or API calls exporting content at unusual hours (T1552.001). Hunt for Kerberos AS-REP Roasting or relay events in AD Security event logs: Event ID 4768 (Kerberos TGT requests) with RC4 encryption type 0x17 from non-standard hosts, and Event ID 4769 (service ticket requests) from unexpected source IPs (T1558.003). Check Azure AD sign-in logs for authentications from on-premises service account UPNs originating from unexpected IPs or user agents (T1550). Review for new scheduled tasks (Event ID 4698, T1053.005) and new accounts created post-initial-access (T1136). Apply D3-LAM (Local Account Monitoring) and D3-SFA (System File Analysis) on affected Linux hosts.

NIST Phase: Detection Analysis

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

Controls: NIST AU-2 (Event Logging), NIST AU-6 (Audit Record Review, Analysis, and Reporting), NIST SI-4 (System Monitoring), NIST IR-5 (Incident Monitoring), CIS 8.2 (Collect Audit Logs)

Compensating: Without SIEM, parse Confluence access logs directly for bulk export IOCs: `grep -E '(GET|POST).*/rest/api/content' /var/atlassian/application-data/confluence/logs/confluence*.log | awk '{print $1, $7}' | sort | uniq -c | sort -rn | head -50` — flag any single IP exceeding 200 page reads within a 1-hour window. For Kerberos hunting without SIEM, run this PowerShell against AD Security logs on each DC: `Get-WinEvent -LogName Security | Where-Object {$_.Id -eq 4768 -and $_.Message -match '0x17'} | Select-Object TimeCreated, Message | Export-Csv kerberos_rc4.csv`. Deploy Sysmon with SwiftOnSecurity config on internal Linux-adjacent Windows hosts and filter EventID 1 for cmd.exe/powershell.exe spawned by the Confluence service account SID. For Azure AD, use the free Microsoft Entra sign-in log export (CSV) filtered on the Confluence service account UPN and sort by IPAddress.

Evidence: Collect Confluence's `confluence-access.log` and `atlassian-confluence.log` from `/var/atlassian/application-data/confluence/logs/` — attacker bulk credential harvesting via T1552.001 leaves sequential REST API calls to `/rest/api/content?type=page&limit=50` with consistent source IP at off-hours. Export Windows Security Event Log from all DCs filtering Event IDs 4768, 4769, 4771, and 4776 for the 30 days preceding discovery — RC4 (etype 0x17) requests from the Confluence server IP are a specific indicator of credential relay setup. Pull Azure AD sign-in logs for the Confluence service account UPN for the same window, specifically hunting `userAgent` fields matching Impacket's default strings (e.g., `python-requests`) or blank user agents indicating non-browser authentication. On internal Linux hosts, collect `/var/log/auth.log` and `/var/log/secure` for SSH authentications originating from the BIG-IP management IP range.

Step 3: Eradication — Replace EOL F5 BIG-IP v15.1.x with a supported version (F5 BIG-IP 17.x or later) or an equivalent supported appliance; no security patch exists for EOL hardware. Apply the MSRC patch for CVE-2025-33073 per the Microsoft Security Advisory

(https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-33073). Apply all outstanding Confluence security patches per Atlassian's current advisory stream. Rotate all service account credentials identified in Confluence pages or configuration exports (D3-CRO, NIST IA-5). Remove embedded credentials from Confluence entirely; enforce secrets management tooling. Reset krbtgt account password twice in AD to invalidate any forged Kerberos tickets (T1558).

NIST Phase: Eradication

Reference: NIST 800-61r3 §3.4 — Eradication

Controls: NIST IA-5 (Authenticator Management), NIST SI-2 (Flaw Remediation), NIST CM-7 (Least Functionality), NIST AC-2 (Account Management), CIS 7.3 (Perform Automated Operating System Patch Management), CIS 7.4 (Perform Automated Application Patch Management), CIS 5.2 (Use Unique Passwords)

Compensating: For krbtgt double-reset without enterprise tooling, use Microsoft's published `New-KrbtgtKeys.ps1` script (available from Microsoft's GitHub) run by a Domain Admin twice with a minimum 10-hour interval between resets to ensure replication completes before the second reset — the 10-hour wait aligns with default AD replication convergence for the Maximum Ticket Lifetime for User Ticket (default 10 hours). To identify embedded credentials in Confluence without a commercial secrets scanner, use truffleHog (open source): `trufflehog filesystem /var/atlassian/application-data/confluence/` against an offline export, or run `grep -rEi '(password|passwd|secret|token|apikey)\s*[:=]\s*\S+' /confluence/export/ > embedded_creds.txt`. For Confluence patching on a minimal team, use Atlassian's documented in-place upgrade path for the specific installed version — do not skip intermediate versions if upgrading across major releases.

Evidence: Before credential rotation, document every service account SPN registered in AD that could have been targeted in the Kerberos relay: `Get-ADUser -Filter {ServicePrincipalName -ne '$null'} -Properties ServicePrincipalName | Select-Object Name, ServicePrincipalName | Export-Csv spn_inventory.csv`. Export Confluence's complete page export for any Space containing IT, infrastructure, credentials, or passwords in the Space name — these are the highest-probability sources of harvested credentials per T1552.001. On the F5 BIG-IP before replacement, extract `/config/bigip.conf` and `/config/bigip_base.conf` and review for any iRules or iCall scripts added or modified after the initial compromise date — these are the primary attacker persistence mechanisms on TMOS. Capture AD replication metadata for the krbtgt account before reset: `repadmin /showattr * CN=krbtgt,CN=Users,DC=domain,DC=com /atts:pwdLastSet`.

Step 4: Recovery — Validate no persistence mechanisms remain: audit scheduled tasks (T1053.005), startup config entries (T1547.005), and DLL search-order hijacking artifacts (T1574.001) on affected Linux and Windows hosts per D3-SICA. Confirm Confluence is running a patched, supported version before reconnecting to internal networks. Verify Azure AD Conditional Access policies block legacy authentication and enforce MFA on all service accounts (CIS 6.3, CIS 6.5, D3-MFA). Re-audit AD for unauthorized accounts or group membership changes created during the intrusion window (NIST AC-2). Monitor for re-exploitation attempts against the replacement perimeter appliance for 30 days post-remediation using enhanced logging per NIST AU-6.

NIST Phase: Recovery

Reference: NIST 800-61r3 §3.5 — Recovery

Controls: NIST AC-2 (Account Management), NIST AU-6 (Audit Record Review, Analysis, and Reporting), NIST CM-6 (Configuration Settings), NIST SI-7 (Software, Firmware, and Information Integrity), CIS 6.3 (Require MFA for Externally-Exposed Applications), CIS 6.5 (Require MFA for Administrative Access)

Compensating: For persistence hunting on Windows hosts without EDR, run Autoruns (Sysinternals) in CLI mode against all affected hosts: `autorunsc.exe -a * -c -h -s > autoruns_$(hostname)_$(date +%F).csv` and diff the output against a known-good baseline. For Linux persistence, check `crontab -l` for all users, `/etc/cron.*`, `/etc/systemd/system/` for new unit files, and `~/.ssh/authorized_keys` for all non-root users — the attacker's SSH lateral movement via T1021.004 frequently deposits authorized_keys entries. For Azure AD legacy auth blocking without an E5 license, use the free Azure AD Sign-in Workbook to identify any service accounts still authenticating via legacy protocols (SMTP AUTH, IMAP, basic auth) and block at the Conditional Access level using the 'Block Legacy Authentication' built-in template available in all Azure AD tiers.

Evidence: Before declaring recovery complete, pull AD audit logs (Event ID 4720 — Account Created, Event ID 4728/4732/4756 — Member Added to Security/Distribution Group) for the full intrusion window scoped to privileged groups: Domain Admins, Enterprise Admins, Schema Admins, and any group with AD replication rights (required for DCSync, T1003.006). On the replacement F5 BIG-IP 17.x, export the initial baseline configuration hash immediately post-deployment for integrity comparison during the 30-day monitoring window. For Confluence, verify the integrity of the `atlassian-confluence.log` timestamp continuity — gaps in log timestamps during the intrusion window may indicate log tampering (NIST AU-9). On Azure AD, export the full Conditional Access policy list and compare against pre-incident baseline to identify any policies disabled or modified during the attacker's Azure access window.

Step 5: Post-Incident — Formalize an EOL asset decommission policy with tracked sunset dates for all perimeter appliances (CIS 2.2, NIST CM-8). Implement a secrets scanning process for Confluence and internal wikis to detect embedded credentials before attackers find them (CWE-522 remediation, NIST IA-5(7)). Enforce least-privilege on all service accounts used by Confluence and adjacent internal applications (NIST AC-6, CIS 5.4). Deploy LLMNR/NBT-NS disable policy via Group Policy to eliminate the Kerberos relay attack surface (T1557.001 mitigation). Conduct a full asset inventory review against EOL schedules quarterly (CIS 1.1, CIS 7.1).

NIST Phase: Post Incident

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

Controls: NIST CM-8 (System Component Inventory), NIST AC-6 (Least Privilege), NIST IA-5 (Authenticator Management), NIST IA-5(7) (No Embedded Unencrypted Static Authenticators), NIST RA-3 (Risk Assessment), CIS 1.1 (Establish and Maintain Detailed Enterprise Asset Inventory), CIS 2.2 (Ensure Authorized Software is Currently Supported), CIS 5.4 (Restrict Administrator Privileges to Dedicated Administrator Accounts), CIS 7.1 (Establish and Maintain a Vulnerability Management Process), CIS 7.2 (Establish and Maintain a Remediation Process)

Compensating: For continuous secrets scanning of Confluence without a commercial tool, schedule a weekly cron job running truffleHog against a Confluence space export: `trufflehog filesystem --json /opt/confluence-exports/ >> /var/log/secrets_scan.log 2>&1`. For LLMNR/NBT-NS disable via GPO: set Computer Configuration > Administrative Templates > Network > DNS Client > 'Turn off multicast name resolution' to Enabled, and set HKLM\SYSTEM\CurrentControlSet\Services\NetBT\Parameters\NodeType to 0x2 (P-node) via GPO registry preference — validate with `Get-WmiObject -Class Win32_NetworkAdapterConfiguration | Select-Object TcpipNetbiosOptions`. For Confluence service account least-privilege, audit the account's AD group memberships with `Get-ADPrincipalGroupMembership -Identity | Select-Object Name` and remove any group beyond what Confluence's documentation explicitly requires for LDAP sync and SSO.

Evidence: For the post-incident lessons-learned report, compile a timeline using the Confluence access log timestamps (T1552.001 harvest window), BIG-IP `/var/log/audit` (initial access window), and AD Event ID 4768/4769 logs (Kerberos relay window) to establish dwell time between initial BIG-IP exploitation and first AD impact — this metric directly informs detection gap analysis per NIST 800-61r3 §4. Preserve the full qkview bundle from the EOL BIG-IP and the Confluence application export as legal-hold artifacts for a minimum of 12 months in case regulatory notification obligations (e.g., state breach laws triggered by credential exposure) require evidence of scope. Document the specific Confluence Spaces and page titles where credentials were found to scope the credential exposure for notification purposes.

Detection Guidance

Primary detection targets span three phases of the attack chain. Phase 1 (Initial Access via F5): Review firewall and SSH logs for connections from the F5 management or data-plane IP range to internal Linux hosts on port 22. Unexpected SSH sessions from perimeter appliances to internal servers are a high-fidelity indicator (T1021.004, T1190). Phase 2 (Credential Harvesting from Confluence): Audit Confluence access logs for service accounts or user accounts performing bulk content reads, REST API exports, or accessing pages tagged with credentials or configuration. Correlate with NIST AU-6 review cadence. Search for T1552.001

indicators: file reads or API calls retrieving configuration files containing plaintext credentials. Phase 3 (Kerberos Relay / AD Attack): In Windows Security event logs, hunt for Event ID 4768 with encryption type 0x17 (RC4) from hosts that are not domain controllers or known service hosts. Event ID 4769 with failure code 0x20 (ticket expired) in bulk may indicate relay or spraying. Event ID 4624 logon type 3 (network logon) from service account UPNs originating from Linux or Confluence host IPs is anomalous. Review Azure AD sign-in logs for on-premises synced accounts authenticating from cloud-only endpoints or unfamiliar ASNs. Apply D3-LAM to detect new local accounts (T1136) and D3-SFA to detect modified SSH authorized_keys or cron entries (T1053.005, T1574.001) on Linux hosts post-access. EPSS score of 0.296 (96.7th percentile) indicates elevated real-world exploitation probability for CVE-2025-33073 specifically.

Indicators of Compromise

Type	Value	Context	Confidence
URL	`https://nvd.nist.gov/vuln/detail/CVE-2025-33073`	NVD entry for CVE-2025-33073, the Kerberos relay vulnerability exploited in this campaign	HIGH
URL	`https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-33073`	Microsoft Security Advisory for CVE-2025-33073 — authoritative patch and mitigation guidance	HIGH

Framework Mappings

MITRE-ATTACK

- **T1572** — Protocol Tunneling
- **T1552.001** — Credentials In Files
- **T1547.005** — Security Support Provider
- **T1071.002** — File Transfer Protocols
- **T1592** — Gather Victim Host Information
- **T1550** — Use Alternate Authentication Material
- **T1558.003** — Kerberoasting
- **T1021.004** — SSH
- **T1557.001** — LLMNR/NBT-NS Poisoning and SMB Relay
- **T1059.004** — Unix Shell
- **T1190** — Exploit Public-Facing Application
- **T1021** — Remote Services
- **T1558** — Steal or Forge Kerberos Tickets
- **T1105** — Ingress Tool Transfer
- **T1003.006** — DCSync
- **T1574.001** — DLL
- **T1552** — Unsecured Credentials

- **T1078** — Valid Accounts
- **T1046** — Network Service Discovery
- **T1136** — Create Account
- **T1210** — Exploitation of Remote Services
- **T1053.005** — Scheduled Task

NIST-800-53R5

- **SC-7** — Boundary Protection
- **CM-7** — Least Functionality
- **SI-3** — Malicious Code Protection
- **SI-4** — System Monitoring
- **CA-8** — Penetration Testing
- **RA-5** — Vulnerability Monitoring and Scanning
- **SI-2** — Flaw Remediation
- **SI-7** — Software, Firmware, and Information Integrity
- **AC-17** — Remote Access
- **AC-3** — Access Enforcement
- **IA-2** — Identification and Authentication (Organizational Users)
- **AC-6** — Least Privilege
- **IA-5** — Authenticator Management
- **CA-7** — Continuous Monitoring
- **AC-2** — Account Management
- **IA-8** — Identification and Authentication (Non-Organizational Users)
- **SI-10** — Information Input Validation
- **IR-5** — Incident Monitoring

OWASP-TOP10-2021

- **A07:2021** — Identification and Authentication Failures
- **A01:2021** — Broken Access Control
- **A04:2021** — Insecure Design
- **A08:2021** — Software and Data Integrity 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
- **5.4** — Restrict Administrator Privileges to Dedicated Administrator Accounts
- **6.8** — Define and Maintain Role-Based Access Control
- **6.1** — Establish an Access Granting Process
- **5.2** — Use Unique Passwords

- **16.10** — Apply Secure Design Principles in Application Architectures
- **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
- **CC6.3** — Authorizes, modifies, or removes access

HIPAA-SECURITY

- **164.312(d)** — Person or Entity Authentication
- **164.308(a)(5)(ii)(D)** — Password Management

ISO-27001-2022

- **A.8.8** — Management of technical vulnerabilities
- **A.5.23** — Information security for use of cloud services

NIST-CSF-2

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

MITRE ATT&CK Mapping

Technique ID	Technique Name	Tactic
T1572	Protocol Tunneling	Command-And-Control
T1552.001	Credentials In Files	Credential-Access
T1547.005	Security Support Provider	Persistence
T1071.002	File Transfer Protocols	Command-And-Control
T1592	Gather Victim Host Information	Reconnaissance
T1550	Use Alternate Authentication Material	Defense-Evasion
T1558.003	Kerberoasting	Credential-Access
T1021.004	SSH	Lateral-Movement
T1557.001	LLMNR/NBT-NS Poisoning and SMB Relay	Credential-Access
T1059.004	Unix Shell	Execution
T1190	Exploit Public-Facing Application	Initial-Access
T1021	Remote Services	Lateral-Movement

Technique ID	Technique Name	Tactic
T1558	Steal or Forge Kerberos Tickets	Credential-Access
T1105	Ingress Tool Transfer	Command-And-Control
T1003.006	DCSync	Credential-Access
T1574.001	DLL	Persistence
T1552	Unsecured Credentials	Credential-Access
T1078	Valid Accounts	Defense-Evasion
T1046	Network Service Discovery	Discovery
T1136	Create Account	Persistence
T1210	Exploitation of Remote Services	Lateral-Movement
T1053.005	Scheduled Task	Execution

Sources

Source	URL	Tier
Microsoft Security Blog	https://www.microsoft.com/en-us/security/blog/2026/05/22/from-edge-...	T1
	https://www.microsoft.com/en-us/security/blog/2026/05/22/from-edge-...	T1
	https://cybersecuritynews.com/f5-big-ip-exploited-for-ssh-access/	T3
	https://www.microsoft.com/en-us/security/blog/2026/02/06/active-exp...	T1
CVE-2025-33073 Detail - NVD	https://nvd.nist.gov/vuln/detail/CVE-2025-33073	T1
Microsoft Security Advisory	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-33073	T1

Generated 2026-05-23 06:27 UTC by TJS Security Command Center