INTELLIGENCE BRIEFING
Security Command Center
TLP:CLEAR
2026-06-18 19:00 UTC

INC Ransomware Reaches 830+ Victims: Rust-Rewritten RaaS Group Targets Downtime-Sensitive Sectors with Expanding Toolkit

THREAT CAMPAIGN | **HIGH** | CVSS 7.5

SCC Item ID	SCC-CAM-2026-0510
Type	Threat Campaign
CVE ID	CVE-2023-3519, CVE-2025-5777, CVE-2023-48788, CVE-2024-57727
Severity	HIGH
CVSS Base Score	7.5
EPSS Score	0.9934 (100th percentile)
Affected Products	Citrix NetScaler ADC/Gateway, Fortinet EMS, SimpleHelp RMM, Veeam Backup & Replication, Windows, Linux/ESXi
Published	2026-06-18T10:12:48
Discovery Source	Rss

Executive Summary

INC Ransomware has grown into the fourth most active ransomware-as-a-service group globally, claiming over 830 victims since August 2023 by exploiting unpatched vulnerabilities in widely deployed enterprise products including Citrix NetScaler, Fortinet EMS, SimpleHelp RMM, and Veeam Backup. The group deliberately targets healthcare, manufacturing, legal, and construction organizations where operational downtime translates directly into ransom leverage. A Rust-based cross-platform encryptor, custom Veeam credential dumper, and driver-based defense evasion signal a maturing threat that may have benefited from 2024 law enforcement actions against LockBit and BlackCat/ALPHV.

Technical Analysis

INC Ransomware (active since August 2023) operates as a RaaS with a Rust-rewritten encryptor targeting Windows and Linux/ESXi environments. Initial access is achieved through exploitation of four disclosed vulnerabilities: CVE-2023-3519 (Citrix NetScaler ADC/Gateway unauthenticated RCE, CVSS 9.8), CVE-2025-5777 (Citrix NetScaler ADC/Gateway), CVE-2023-48788 (Fortinet EMS SQL injection leading to RCE, CVSS 9.8), and CVE-2024-57727 (SimpleHelp RMM path traversal enabling unauthenticated file read).

Post-access, the group deploys a custom credential dumper against Veeam Backup & Replication (targeting backup authentication stores), uses Bring Your Own Vulnerable Driver (BYOVD) techniques to disable endpoint detection and response tools (T1562.001, CWE-269), and moves laterally via RDP (T1021.001) and remote services (T1021). Encryption is paired with data exfiltration (T1560, T1041) for double extortion. Relevant CWEs include CWE-287 (improper authentication), CWE-89 (SQL injection), CWE-78 (OS command injection), CWE-22 (path traversal), CWE-522 (insufficiently protected credentials), CWE-269 (improper privilege management), and CWE-494 (download of code without integrity check). EPSS score of 0.993 places the associated CVEs in the 99.9th percentile of exploitation likelihood. No CISA KEV listing is recorded in the provided data for this campaign item. Note: CVE-2023-3519 may have KEV status; verify current KEV status at cisa.gov.

Action Checklist

1. Step 1: Containment, Immediately audit internet-facing Citrix NetScaler ADC/Gateway instances for CVE-2023-3519 and CVE-2025-5777 exposure; isolate unpatched appliances from production until patches are applied. Audit Fortinet EMS deployments for CVE-2023-48788 exposure and apply Fortinet's available patch. Identify any SimpleHelp RMM installations and restrict external access pending CVE-2024-57727 remediation. Reference vendor advisories: Citrix CTX561482 for CVE-2023-3519 and Censys advisory for CVE-2025-5777. Map NIST SI-4 (system monitoring) controls to confirm perimeter visibility on these assets.
2. Step 2: Detection, Query EDR and SIEM for BYOVD indicators: unexpected driver loads from non-standard paths, termination of EDR agent processes, and Service Control Manager events (Windows Event ID 7045) for unknown drivers. Review NetScaler access logs for anomalous POST requests to /vpns/ and /oauth/idp/ endpoints associated with CVE-2023-3519 exploitation. Hunt for INC-associated MITRE techniques: T1190 (exploit public-facing application), T1003 (credential dumping against Veeam processes), T1562.001 (impair defenses), T1486 (data encryption for impact), and T1041 (exfiltration over C2). Check Veeam Backup & Replication logs for unexpected authentication attempts or service account access. Apply NIST AU-6 (audit record review and analysis). Reference D3-LAM (Local Account Monitoring) and D3-SFA (System File Analysis) countermeasures.
3. Step 3: Eradication, Apply all available patches: Citrix NetScaler patches for CVE-2023-3519 and CVE-2025-5777 per CTX561482 and current Citrix security bulletins; Fortinet EMS patch for CVE-2023-48788 per Fortinet advisory; SimpleHelp patch for CVE-2024-57727 per vendor release notes. Rotate all service account credentials exposed through Veeam or compromised RMM sessions (D3-CRO). Remove any unauthorized drivers loaded via BYOVD technique. Audit and enforce allowlisting of signed drivers only. Apply NIST CM controls to validate configuration integrity post-patch. Enforce CIS 7.3 and CIS 7.4 (automated OS and application patch management) to close recurring patch gaps.
4. Step 4: Recovery, After patching, validate remediation by re-scanning affected systems with an authenticated vulnerability scanner targeting the four CVEs. Confirm EDR agents are running and reporting on all endpoints, particularly those where BYOVD was suspected. Restore Veeam backup integrity by verifying backup chain authenticity and rotating all backup service credentials. Monitor for re-exploitation attempts against the patched surfaces for a minimum of 30 days. Apply NIST AU-12 (audit record generation) to ensure logging is active across restored systems. Validate MFA enforcement on all remote access paths per CIS 6.4.
5. Step 5: Post-Incident, Conduct a control gap review against CIS 7.1 (vulnerability management process) and CIS 7.2 (risk-based remediation strategy) to determine why CVE-2023-3519 (disclosed July

2023) remained exploitable in INC campaigns through 2025-2026. Evaluate whether BYOVD defenses (driver allowlisting, Vulnerable Driver Blocklist per Microsoft guidance) are implemented. Assess backup segmentation: Veeam targeting indicates backup infrastructure is reachable from compromised hosts, apply network segmentation controls (NIST AC-4, information flow enforcement) to isolate backup systems. Review RDP exposure and enforce NIST AC-17 (remote access policy) with MFA requirements (D3-MFA). Develop or update ransomware-specific incident response playbooks referencing the INC kill chain.

IR / Forensic Enrichment

Triage Priority	IMMEDIATE
Escalation Criteria	Escalate to CISO, legal counsel, and external IR retainer immediately if: (1) any NetScaler, Fortinet EMS, or SimpleHelp appliance shows confirmed exploitation indicators (webshell presence, anomalous POST to /vpns/ or /oauth/idp/, unauthorized SQL execution in Fortinet EMS); (2) Veeam backup service account shows evidence of access outside normal backup windows; (3) any Windows host shows Event ID 7045 for an unrecognized driver — indicating BYOVD and probable INC encryptor pre-staging; or (4) the organization operates in healthcare or critical infrastructure where HIPAA breach notification or CISA mandatory reporting obligations may be triggered by confirmed data exfiltration.
Recovery Notes	Do not return NetScaler, Fortinet EMS, or SimpleHelp RMM to production until authenticated vulnerability scans confirm all four CVEs are remediated and no webshells or backdoor accounts remain on the appliances. Veeam backup infrastructure must be treated as potentially compromised until backup chain integrity is cryptographically verified and all service credentials rotated — INC specifically targets backup systems to maximize ransom leverage by eliminating recovery options. Monitor all four previously vulnerable surfaces continuously for re-exploitation attempts for a minimum of 30 days post-recovery, with specific alerting on the NetScaler /vpns/ and /oauth/idp/ URI patterns and Windows Event ID 7045 for new driver installs, given INC's demonstrated persistence and the 830+ victim scale indicating active, resourced operations.
Forensic Artifacts	NetScaler /var/nslog/httprequest.log and /var/nslog/ns.log: contains POST requests to /vpns/ and /oauth/idp/ endpoints that are the primary exploitation signatures for CVE-2023-3519; timestamp correlation with subsequent host compromise events establishes the initial access timeline | Windows Registry hive HKLM\SYSTEM\CurrentControlSet\Services\: INC's BYOVD technique creates new service entries for the vulnerable driver used to terminate EDR agents; registry forensics on this hive before and after the intrusion window identifies the specific driver name, binary path, and installation timestamp | Veeam Backup & Replication SQL database (VeeamBackup on local SQL instance): contains authentication history, job execution records, and credential references; INC access to this database indicates backup infrastructure compromise and establishes scope of potential data exfiltration from backup-stored sensitive data | Windows Security Event Log (Event ID 7045 — Service Installed, Event ID 4624/4648 — Logon/Explicit Credential Use): Event ID 7045 is the primary host-based indicator of INC's BYOVD driver installation; Event ID 4624/4648 on the Veeam server scoped to the VeeamBackup service account identifies the credential access phase of the INC attack chain | Memory acquisition (WinPmem/DumpIt) from hosts where INC Rust encryptor execution is suspected: the cross-platform Rust encryptor may exist only in memory during early staging before writing encrypted files; memory forensics with Volatility using the `malfind` and `cmdline` plugins recovers encryptor process artifacts, injected code, and in-memory C2 configuration not present in on-disk artifacts

Per-Action IR Details

Step 1: Containment — Immediately audit internet-facing Citrix NetScaler ADC/Gateway instances for CVE-2023-3519 and CVE-2025-5777 exposure; isolate unpatched appliances from production until patches are applied. Audit Fortinet EMS deployments for CVE-2023-48788 exposure and apply Fortinet's available patch. Identify any SimpleHelp RMM installations and restrict external access pending CVE-2024-57727 remediation. Reference vendor advisories: Citrix CTX561482 for CVE-2023-3519 and Censys advisory for CVE-2025-5777 (URLs provided in source data). Map NIST SI-4 (system monitoring) controls to confirm perimeter visibility on these assets.

NIST Phase: Containment

Reference: NIST 800-61r3 §3.3 — Containment Strategy: isolate affected systems to prevent INC lateral movement from compromised NetScaler, Fortinet EMS, or SimpleHelp RMM footholds into the internal environment

Controls: NIST AC-4 (Information Flow Enforcement), NIST AC-17 (Remote Access), CIS 4.4 (Implement and Manage a Firewall on Servers), CIS 7.1 (Establish and Maintain a Vulnerability Management Process)

Compensating: For teams without NAC or enterprise firewall orchestration: use Windows Firewall (`netsh advfirewall firewall add rule`) or iptables (`iptables -I INPUT -s -j DROP`) to block inbound traffic to unpatched appliances. Run a Nmap authenticated scan (`nmap -sV --script=citrix-enum-apps`) against NetScaler management IPs to confirm version exposure. For SimpleHelp, disable the Windows service (`sc stop SimpleHelp` / `sc config SimpleHelp start= disabled`) until patched. Document every isolated asset in a timestamped incident log.

Evidence: BEFORE isolating any NetScaler or Fortinet EMS appliance, capture: (1) full NetScaler ns.log and /var/nslog/ directory contents showing active sessions and recent POST requests to /vpns/ and /oauth/idp/ endpoints; (2) Fortinet EMS database query logs and /var/log/FortiClientEMS/ for anomalous SQL traffic indicative of CVE-2023-48788 SQL injection exploitation; (3) SimpleHelp server logs at /logs/ for unauthorized session establishment or credential harvesting activity; (4) active TCP connection state via `netstat -ano` or `ss -tulnp` on each appliance before network isolation to capture C2 channel endpoints.

Step 2: Detection — Query EDR and SIEM for BYOVD indicators: unexpected driver loads from non-standard paths, termination of EDR agent processes, and Service Control Manager events (Windows Event ID 7045) for unknown drivers. Review NetScaler access logs for anomalous POST requests to /vpns/ and /oauth/idp/ endpoints associated with CVE-2023-3519 exploitation. Hunt for INC-associated MITRE techniques: T1190 (exploit public-facing application), T1003 (credential dumping against Veeam processes), T1562.001 (impair defenses), T1486 (data encryption for impact), and T1041 (exfiltration over C2). Check Veeam Backup & Replication logs for unexpected authentication attempts or service account access. Apply NIST AU-6 (audit record review and analysis). Reference D3-LAM (Local Account Monitoring) and D3-SFA (System File Analysis) countermeasures.

NIST Phase: Detection Analysis

Reference: NIST 800-61r3 §3.2 — Detection and Analysis: correlate NetScaler exploitation telemetry with host-based BYOVD driver load events and Veeam credential access patterns to scope INC's lateral movement chain and determine blast radius before declaring incident severity

Controls: NIST AU-6 (Audit Record Review, Analysis, And Reporting), NIST AU-2 (Event Logging), NIST AU-12 (Audit Record Generation), CIS 8.2 (Collect Audit Logs)

Compensating: Deploy Sysmon with a community config (SwiftOnSecurity or Olaf Hartong) to capture Event ID 6 (driver loaded) and Event ID 1 (process creation) for EDR-kill activity. Run `Get-WinEvent -LogName System | Where-Object {$_.Id -eq 7045}` on all Windows endpoints to surface unknown driver installs. For NetScaler log analysis without SIEM, use `grep -E 'POST.*/vpns/|POST.*/oauth/idp/' /var/nslog/httprequest.log` to surface CVE-2023-3519 exploitation attempts. Use osquery (`SELECT * FROM drivers WHERE signed = '0';`) to enumerate unsigned driver loads. For Veeam, query Windows Security Event Log on the Veeam server for Event ID 4624 (logon) and 4648 (explicit credential use) filtering on the VeeamBackup service account.

Evidence: Volatile evidence to capture BEFORE any process termination or host isolation: (1) full RAM acquisition from any Windows host where BYOVD is suspected using WinPmem or DumpIt — INC's Rust encryptor and BYOVD driver artifacts exist only in memory until written to disk; (2) `Get-NetTCPConnection` and `netstat -ano` output capturing active C2 connections established post-NetScaler exploitation; (3) live process list (`tasklist /v` or `Get-Process`) to identify INC encryptor process names and parent-child relationships indicating lateral tool execution; (4) Windows Security Event Log exported from Veeam server before credential rotation to preserve Event ID 4624/4648 logon chain; (5) NetScaler /var/crash/ and /var/core/ directories for any crash artifacts from CVE-2023-3519 exploitation attempts.

Step 3: Eradication — Apply all available patches: Citrix NetScaler patches for CVE-2023-3519 and CVE-2025-5777 per CTX561482 and current Citrix security bulletins; Fortinet EMS patch for CVE-2023-48788 per Fortinet advisory; SimpleHelp patch for CVE-2024-57727 per vendor release notes. Rotate all service account credentials exposed through Veeam or compromised RMM sessions (D3-CRO). Remove any unauthorized drivers loaded via BYOVD technique. Audit and enforce allowlisting of signed drivers only. Apply NIST CM controls to validate configuration integrity post-patch. Enforce CIS 7.3 and CIS 7.4 (automated OS and application patch management) to close recurring patch gaps.

NIST Phase: Eradication

Reference: NIST 800-61r3 §3.4 — Eradication: remove INC persistence mechanisms including BYOVD drivers and unauthorized RMM sessions, patch all four CVEs exploited in the INC kill chain, and verify no backdoor accounts remain before returning systems to production

Controls: NIST AC-2 (Account Management), NIST AC-6 (Least Privilege), CIS 7.3 (Perform Automated Operating System Patch Management), CIS 7.4 (Perform Automated Application Patch Management), CIS 4.6 (Securely Manage Enterprise Assets and Software)

Compensating: For driver allowlisting without a commercial solution, configure Windows Defender Application Control (WDAC) using the Microsoft Recommended Driver Block Rules policy deployed via Group Policy or PowerShell (`Set-CIPolicy`). Enumerate all loaded drivers before and after eradication with `driverquery /v /fo csv > drivers_baseline.csv` and diff the outputs. For credential rotation verification, run `net user /domain` and audit Active Directory for newly created accounts or accounts with `PasswordLastSet` timestamps coinciding with the INC intrusion window using `Get-ADUser -Filter * -Properties PasswordLastSet`. Remove unauthorized SimpleHelp sessions via the admin console and revoke all session tokens by restarting the service after credential rotation.

Evidence: BEFORE applying any patch, rotating credentials, or removing BYOVD drivers: (1) acquire a full disk image or forensic copy of any host where an INC BYOVD driver was identified — the driver binary on disk and its associated INF/registry entries under `HKLM\SYSTEM\CurrentControlSet\Services\` are primary forensic artifacts; (2) export the registry hive `HKLM\SYSTEM\CurrentControlSet\Services` to capture driver service entries created by INC's BYOVD technique before they are removed; (3) collect Veeam Backup & Replication configuration database (`VeeamBackup` SQL database backup) and credential store artifacts before service account rotation to preserve the compromise scope; (4) document all active SimpleHelp session tokens and connection logs before service restart.

Step 4: Recovery — After patching, validate remediation by re-scanning affected systems with an authenticated vulnerability scanner targeting the four CVEs. Confirm EDR agents are running and reporting on all endpoints, particularly those where BYOVD was suspected. Restore Veeam backup integrity by verifying backup chain authenticity and rotating all backup service credentials. Monitor for re-exploitation attempts against the patched surfaces for a minimum of 30 days. Apply NIST AU-12 (audit record generation) to ensure logging is active across restored systems. Validate MFA enforcement on all remote access paths per CIS 6.4.

NIST Phase: Recovery

Reference: NIST 800-61r3 §3.5 — Recovery: restore operational capability for NetScaler, Fortinet EMS, SimpleHelp, and Veeam only after authenticated vulnerability validation confirms all four INC-exploited CVEs are remediated and backup chain integrity is verified

Controls: NIST AU-12 (Audit Record Generation), NIST AU-6 (Audit Record Review, Analysis, And Reporting), CIS 6.4 (Require MFA for Remote Network Access), CIS 6.3 (Require MFA for Externally-Exposed Applications), CIS 8.2 (Collect Audit Logs)

Compensating: Use OpenVAS or Greenbone Community Edition with authenticated scan policies targeting CVE-2023-3519, CVE-2025-5777, CVE-2023-48788, and CVE-2024-57727 to validate patch application without a commercial scanner. Verify Veeam backup chain integrity using Veeam's built-in `Start-VBRRestorePointSizeRecalculation` and `Get-VBRBackup` PowerShell cmdlets to confirm no backup files were encrypted or tampered. For MFA validation on RDP paths, audit Group Policy Object `Computer Configuration > Windows Settings > Security Settings > Account Policies` and verify Network Level Authentication is enforced. Monitor NetScaler `/vpns/` and `/oauth/idp/` endpoints post-recovery using a YARA rule on web access logs for 30 days.

Evidence: Before returning any system to production, capture: (1) authenticated vulnerability scan report confirming CVE-2023-3519, CVE-2025-5777, CVE-2023-48788, and CVE-2024-57727 are no longer present on the respective appliances — this serves as the formal remediation closure artifact; (2) Veeam backup job completion logs and SHA-256 hash verification of restored backup files to confirm INC's encryptor did not corrupt the backup chain before containment; (3) EDR agent health report confirming all endpoints — particularly those where BYOVD driver termination of security tools was suspected — have restored, communicating agents with no gaps in telemetry coverage.

Step 5: Post-Incident — Conduct a control gap review against CIS 7.1 (vulnerability management process) and CIS 7.2 (risk-based remediation strategy) to determine why CVE-2023-3519 (disclosed July 2023) remained exploitable in INC campaigns through 2025-2026. Evaluate whether BYOVD defenses (driver allowlisting, Vulnerable Driver Blocklist per Microsoft guidance) are implemented. Assess backup segmentation: Veeam targeting indicates backup infrastructure is reachable from compromised hosts — apply network segmentation controls (NIST AC-4, information flow enforcement) to isolate backup systems. Review RDP exposure and enforce NIST AC-17 (remote access policy) with MFA requirements (D3-MFA). Develop or update ransomware-specific incident response playbooks referencing the INC kill chain.

NIST Phase: Post Incident

Reference: NIST 800-61r3 §4 — Post-Incident Activity: document the INC kill chain from initial NetScaler/Fortinet EMS exploitation through BYOVD defense evasion to Veeam backup targeting and Rust encryptor deployment; update IR playbooks and patch SLAs to prevent recurrence of a 2+ year exploitation window on CVE-2023-3519

Controls: NIST AC-4 (Information Flow Enforcement), NIST AC-17 (Remote Access), CIS 7.1 (Establish and Maintain a Vulnerability Management Process), CIS 7.2 (Establish and Maintain a Remediation Process), CIS 4.2 (Establish and Maintain a Secure Configuration Process for Network Infrastructure)

Compensating: For organizations without a GRC platform, conduct the control gap review using a CIS Controls v8 self-assessment spreadsheet (freely available from CIS) scored against the four INC-exploited CVE remediation timelines. Document patch SLA breaches in a risk register. For backup network segmentation without VLAN capability, implement host-based firewall rules on the Veeam server using Windows Firewall with Advanced Security to allow inbound connections only from explicitly authorized backup proxies and management hosts (`netsh advfirewall firewall add rule name='Veeam Allow' dir=in action=allow remoteip=`). Publish a Sigma rule for INC's NetScaler POST exploitation pattern to your log pipeline for ongoing detection.

Evidence: Post-incident artifacts to preserve for lessons-learned and regulatory purposes: (1) complete timeline reconstruction from NetScaler /var/nslog/ access logs through Windows Security Event Log showing the full INC intrusion chain from initial exploitation to encryptor execution; (2) forensic copy of any BYOVD driver binary recovered from disk or memory for malware analysis and IOC extraction; (3) patch management records showing when CVE-2023-3519 (July 2023) and other INC-exploited CVEs were assessed, prioritized, and why remediation was deferred — this is the primary artifact for regulatory inquiry and internal accountability review; (4) Veeam backup access audit log showing which accounts accessed backup infrastructure during the intrusion window, supporting determination of data exposure scope.

Detection Guidance

Priority detection targets for INC Ransomware activity, mapped to MITRE ATT&CK and observable log sources:

1. Initial Access (T1190): Alert on anomalous HTTP POST requests to Citrix NetScaler /vpns/ and /oauth/idp/ paths. Monitor Fortinet EMS logs for SQL error patterns or unexpected system command execution in application logs. Review SimpleHelp server logs for unauthenticated path traversal attempts (../ sequences in file request logs).

2. Defense Evasion / BYOVD (T1562.001): Windows Security Event ID 7045 (new service installed) for drivers loaded from user-writable or temp directories. EDR telemetry for known vulnerable driver hashes (e.g., RTCore64.sys, DBUtil_2_3.sys, and other LOLBAS drivers on the MSFT Vulnerable Driver Blocklist). Alert on EDR process termination events not initiated by authorized management tools.

3. Credential Dumping (T1003): LSASS memory access from non-system processes. Veeam-specific: monitor VeeamBackup database access from unexpected service accounts; alert on Veeam configuration export or credential export API calls outside maintenance windows.

4. Lateral Movement (T1021.001): RDP connections from non-administrative source hosts, especially from NetScaler or EMS server segments. Logins using service accounts on workstations or servers where those accounts have no legitimate interactive use.

5. Encryption and Impact (T1486, T1485, T1489): File rename storms with extensions not on known-good allowlists. Shadow copy deletion: Windows Event ID 524, vssadmin.exe or wmic.exe invocation with 'shadowcopy delete' arguments. Service stop/disable commands targeting backup agents and AV services (T1489).

6. Exfiltration (T1041, T1560): Unusual outbound data volumes from servers hosting Veeam or backup data. Archive creation (7zip, WinRAR) in non-standard paths, followed by outbound HTTPS connections to non-categorized or newly registered domains.

Control references: NIST AU-6 (audit record review), NIST SI-4 (system monitoring). D3FEND: D3-LAM (Local Account Monitoring), D3-SFA (System File Analysis), D3-UAP (User Account Permissions).

Indicators of Compromise

Type	Value	Context	Confidence
URL	`https://thehackernews.com/2026/06/inc-ransomware-claims-830-victims-since.html`	Source reporting on INC Ransomware campaign reaching 830+ victims — T3 source, human validation recommended	LOW
URL	`https://nvd.nist.gov/vuln/detail/cve-2023-3519`	NVD entry for CVE-2023-3519 — Citrix NetScaler unauthenticated RCE exploited by INC for initial access	HIGH
URL	`https://censys.com/advisory/cve-2025-5777-cve-2025-6543-cve-2025-5439/`	Censys advisory covering CVE-2025-5777 and related NetScaler vulnerabilities — T3 source, human validation recommended	LOW

Framework Mappings

MITRE-ATTACK

- **T1485** — Data Destruction
- **T1083** — File and Directory Discovery
- **T1068** — Exploitation for Privilege Escalation
- **T1003** — OS Credential Dumping
- **T1190** — Exploit Public-Facing Application
- **T1486** — Data Encrypted for Impact
- **T1560** — Archive Collected Data
- **T1566.001** — Spearphishing Attachment
- **T1489** — Service Stop
- **T1059** — Command and Scripting Interpreter
- **T1021.001** — Remote Desktop Protocol
- **T1569.002** — Service Execution
- **T1570** — Lateral Tool Transfer
- **T1219** — Remote Access Tools
- **T1071** — Application Layer Protocol
- **T1078** — Valid Accounts
- **T1082** — System Information Discovery
- **T1491** — Defacement
- **T1021** — Remote Services
- **T1041** — Exfiltration Over C2 Channel
- **T1562.001** — Disable or Modify Tools

NIST-800-53R5

- **AC-6** — Least Privilege
- **SC-7** — Boundary Protection
- **SI-2** — Flaw Remediation
- **IA-5** — Authenticator Management
- **SI-4** — System Monitoring
- **CA-8** — Penetration Testing
- **RA-5** — Vulnerability Monitoring and Scanning
- **SI-7** — Software, Firmware, and Information Integrity
- **CP-9** — System Backup
- **CP-10** — System Recovery and Reconstitution
- **AT-2** — Literacy Training and Awareness
- **SI-3** — Malicious Code Protection
- **SI-8** — Spam Protection
- **CM-6** — Configuration Settings
- **CM-7** — Least Functionality

- **CA-7** — Continuous Monitoring
- **AC-2** — Account Management
- **IA-2** — Identification and Authentication (Organizational Users)
- **AC-17** — Remote Access
- **AC-3** — Access Enforcement
- **IA-8** — Identification and Authentication (Non-Organizational Users)
- **SI-10** — Information Input Validation
- **CM-3** — Configuration Change Control
- **IR-4** — Incident Handling
- **SC-13** — Cryptographic Protection

OWASP-TOP10-2021

- **A07:2021** — Identification and Authentication Failures
- **A03:2021** — Injection
- **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
- **16.10** — Apply Secure Design Principles in Application Architectures
- **2.5** — Allowlist Authorized Software
- **16.12** — Implement Code-Level Security Checks
- **5.2** — Use Unique Passwords
- **5.4** — Restrict Administrator Privileges to Dedicated Administrator Accounts
- **6.8** — Define and Maintain Role-Based Access Control
- **2.6** — Allowlist Authorized Libraries

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)(5)(ii)(D)** — Password Management
- **164.308(a)(7)(ii)(A)** — Data Backup Plan
- **164.312(e)(1)** — Transmission Security

ISO-27001-2022

- **A.8.28** — Secure coding

- **A.5.29** — Information security during disruption
- **A.8.8** — Management of technical vulnerabilities
- **A.8.24** — Use of cryptography

NIST-CSF-2

- **RS.MI-01** — Incidents are contained

MITRE ATT&CK Mapping

Technique ID	Technique Name	Tactic
T1485	Data Destruction	Impact
T1083	File and Directory Discovery	Discovery
T1068	Exploitation for Privilege Escalation	Privilege-Escalation
T1003	OS Credential Dumping	Credential-Access
T1190	Exploit Public-Facing Application	Initial-Access
T1486	Data Encrypted for Impact	Impact
T1560	Archive Collected Data	Collection
T1566.001	Spearphishing Attachment	Initial-Access
T1489	Service Stop	Impact
T1059	Command and Scripting Interpreter	Execution
T1021.001	Remote Desktop Protocol	Lateral-Movement
T1569.002	Service Execution	Execution
T1570	Lateral Tool Transfer	Lateral-Movement
T1219	Remote Access Tools	Command-And-Control
T1071	Application Layer Protocol	Command-And-Control
T1078	Valid Accounts	Defense-Evasion
T1082	System Information Discovery	Discovery
T1491	Defacement	Impact
T1021	Remote Services	Lateral-Movement
T1041	Exfiltration Over C2 Channel	Exfiltration
T1562.001	Disable or Modify Tools	Defense-Evasion

Sources

Source	URL	Tier
Security News	https://thehackernews.com/2026/06/inc-ransomware-claims-830-victims...	T3
CVE-2023-3519 Detail - NVD	https://nvd.nist.gov/vuln/detail/cve-2023-3519	T1
Citrix ADC and Citrix Gateway Security Bulletin for CVE-2023-3519 ...	https://support.citrix.com/external/article/CTX561482/citrix-adc-an...	T3
Multiple Vulnerabilities in NetScaler Gateway & ADC [CVE-2025 ...	https://censys.com/advisory/cve-2025-5777-cve-2025-6543-cve-2025-5439/	T3
Analysis of CVE-2023-3519 in Citrix ADC and NetScaler Gateway ...	https://www.assetnote.io/resources/research/analysis-of-cve-2023-35...	T3
NVD	https://nvd.nist.gov/vuln/detail/CVE-2023-3519, CVE-2025-5777, CVE-...	T1

Generated 2026-06-18 19:00 UTC by TJS Security Command Center