INTELLIGENCE BRIEFING
Security Command Center

TLP:CLEAR
2026-03-29 18:44 UTC

Recommendation for CVE■2026■3055

CVE VULNERABILITY | MEDIUM

SCC Item ID	SCC-CVE-2026-0026
Type	CVE Vulnerability
Severity	MEDIUM
Published	2026-03-23
Discovery Source	Serper

Executive Summary

On March 23, 2026, Citrix released patches for CVE-2026-3055, a critical out-of-bounds read vulnerability in NetScaler ADC and NetScaler Gateway. Organizations running unpatched NetScaler appliances face risk of information disclosure or potential service disruption if the vulnerability is exploited by external or internal threat actors. Immediate patching is the required action; no workaround substitutes for the vendor fix.

Technical Analysis

CVE-2026-3055 is an out-of-bounds read vulnerability affecting Citrix NetScaler ADC and NetScaler Gateway. The vulnerability was disclosed and patched by Citrix on March 23, 2026, via security bulletin CTX696300. An out-of-bounds read condition allows an attacker to read memory beyond allocated buffer boundaries, which can expose sensitive data in process memory or contribute to service instability. Full affected version ranges, CVSS scoring, and CWE classification are available in the NVD entry (https://nvd.nist.gov/vuln/detail/CVE-2026-3055) and the Citrix bulletin (https://support.citrix.com/support-home/kbsearch/article?articleNumber=CTX696300). No CVSS score or vector was present in the source data provided for this item; consult NVD and the Citrix bulletin directly for current scoring. No CISA KEV listing was recorded at the time of this item's generation. A companion vulnerability, CVE-2026-4368, was also addressed in CTX696300 and should be patched concurrently. No confirmed active exploitation or public proof-of-concept code was identified in the provided source data.

Action Checklist

1. Step 1: Containment. Identify all NetScaler ADC and NetScaler Gateway appliances in your environment, including cloud and on-premises instances. Restrict management interface access to trusted IP ranges via ACL if patching cannot be completed immediately. Reference Citrix bulletin CTX696300 for affected version identification.

2. Step 2: Detection. Query NetScaler system logs and SIEM for anomalous memory fault events, unexpected process crashes, or elevated error rates on NetScaler services. Review NetScaler Console Service advisory telemetry if deployed (https://docs.netscaler.com/en-us/netscaler-console-service/instance-advisory/remediate-vulnerabilities-cve-2026-3055). Check for any unexpected data in responses from Gateway or ADC services that may indicate memory leakage.
3. Step 3: Eradication. Apply the vendor-issued patch documented in CTX696300. Follow the version-specific upgrade path provided in the Citrix bulletin. Patch CVE-2026-4368 in the same maintenance window. Confirm patch application via NetScaler CLI version verification command and NetScaler Console Service vulnerability scan.
4. Step 4: Recovery. After patching, verify NetScaler ADC and Gateway services are operating normally. Re-run the NetScaler Console Service vulnerability assessment to confirm CVE-2026-3055 and CVE-2026-4368 are no longer flagged. Monitor application delivery and authentication logs for anomalies for at least 72 hours post-patch.
5. Step 5: Post-Incident. Evaluate patch cadence for network edge appliances; Citrix NetScaler has had recurring critical CVEs. Confirm that NetScaler management interfaces are not internet-exposed. Document this patching event in your vulnerability management record and review whether automated advisory alerting for Citrix products is in place.

IR / Forensic Enrichment

Triage Priority	URGENT
Escalation Criteria	Escalate to incident commander and engage Citrix support if any evidence of pre-patch exploitation is found — specifically core dumps in /var/core/, unexpected memory content in Gateway HTTP responses, or authentication anomalies in /var/nslog/ns.log — as these conditions indicate active exploitation of CVE-2026-3055 and potential information disclosure requiring breach notification assessment.
Recovery Notes	After patching both CVE-2026-3055 and CVE-2026-4368 in the same maintenance window, verify all NetScaler ADC and Gateway virtual servers return to 'UP' state and confirm no memory fault events appear in /var/nslog/ns.log for 72 hours post-patch. If NetScaler Gateway is used for remote access to regulated data (PII, PHI, financial records), assess whether any pre-patch requests returned anomalous response payloads that could constitute an information disclosure event warranting regulatory notification. Retain all pre-patch log captures and response samples for a minimum of 90 days in case disclosure scope assessment is required.

Forensic Artifacts	/var/nslog/ns.log — Primary NetScaler system log; contains process crash events, memory fault indicators (segfault, core dump strings), and authentication events that would evidence CVE-2026-3055 out-of-bounds read triggering or exploitation attempts against Gateway/ADC services. | /var/core/ directory — Core dump files generated when a NetScaler process crashes due to memory fault conditions; presence of core dumps timestamped prior to patching is direct forensic evidence of the out-of-bounds read condition described in CVE-2026-3055. | Raw HTTP/HTTPS response captures from Gateway VPN/authentication endpoints — Anomalous trailing data or content exceeding expected response lengths in captures from /vpn/index.html or /cgi/login endpoints would indicate memory content leakage to external requestors, constituting evidence of information disclosure. | 'show ns ip' and 'show version' CLI output snapshots — Establishes the exact affected firmware build and NSIP exposure posture at time of incident, required for CTX696300 affected version correlation and regulatory disclosure scope determination. | Firewall and network flow logs for TCP 443/80 to NetScaler NSIP addresses — Anomalous source IPs or high request volumes to management interfaces in the period preceding patch application may indicate reconnaissance or exploitation of CVE-2026-3055 from external threat actors.

Per-Action IR Details

Step 1: Containment — Identify all NetScaler ADC and NetScaler Gateway appliances in your environment, including cloud and on-premises instances. Restrict management interface access to trusted IP ranges via ACL if patching cannot be completed immediately. Reference Citrix bulletin CTX696300 for affected version identification.

NIST Phase: Containment

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

Controls: NIST IR-4 (Incident Handling), NIST SC-7 (Boundary Protection), CIS 1.1 (Establish and Maintain Detailed Enterprise Asset Inventory), CIS 4.4 (Implement and Manage a Firewall on Servers)

Compensating: Run 'show ns ip' on each NetScaler CLI to enumerate all deployed appliances and confirm running firmware version against CTX696300's affected version table. For teams without a CMDB, cross-reference DNS records and firewall rules for known NetScaler management ports (TCP 80/443/22/3010). Apply ACL blocking non-trusted source IPs to the NSIP (management IP) using 'add ns acl BLOCK_MGMT DENY -srcIP -destIP ' then 'apply ns acls' — this survives reboots and does not require enterprise tools.

Evidence: Before applying ACLs, capture the current NetScaler NSIP and SNIP configuration via 'show ns ip' and 'show ns config' and preserve the output. Export existing ACL rules via 'show ns acl' so pre-containment access policy is documented. Record the running firmware build via 'show version' for each appliance to confirm exact affected build per CTX696300.

Step 2: Detection — Query NetScaler system logs and SIEM for anomalous memory fault events, unexpected process crashes, or elevated error rates on NetScaler services. Review NetScaler Console Service advisory telemetry if deployed (https://docs.netscaler.com/en-us/netscaler-console-service/instance-advisory/remediate-vulnerabilities-cve-2026-3055). Check for any unexpected data in responses from Gateway or ADC services that may indicate memory leakage.

NIST Phase: Detection Analysis

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

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

Compensating: On the NetScaler CLI, run 'show audit messages' and 'show process' to surface unexpected crashes or respawning daemons (particularly the nsppe, nsvpn, or nsaaad processes associated with ADC/Gateway functions). Parse /var/nslog/ns.log for 'segfault', 'core dump', 'out of bounds', or 'memory fault' strings using: grep -iE 'segfault|core dump|out of bounds|memory fault' /var/nslog/ns.log. For memory leak indicators in HTTP responses, capture Gateway

SSL VPN or authentication endpoint responses with curl and inspect for anomalous trailing data or malformed headers: curl -v https:///vpn/index.html > response_dump.txt 2>&1. If Wireshark/tcpdump is available, capture traffic on the Gateway virtual server IP and filter for HTTP responses exceeding expected content-length boundaries.

Evidence: Collect /var/nslog/ns.log and /var/log/messages from each NetScaler appliance before any restart or patch operation — these are overwritten on reboot. Preserve core dump files from /var/core/ if present, as they would confirm memory fault conditions consistent with CVE-2026-3055 out-of-bounds read triggering. Capture raw HTTP/HTTPS response payloads from Gateway authentication endpoints to detect memory content leakage in server responses. Note: the URL provided in the advisory step references Citrix documentation — verify it resolves correctly in your environment before relying on it; human validation of that URL is recommended.

Step 3: Eradication — Apply the vendor-issued patch documented in CTX696300. Follow the version-specific upgrade path provided in the Citrix bulletin. Patch CVE-2026-4368 in the same maintenance window. Confirm patch application via NetScaler CLI version verification command and NetScaler Console Service vulnerability scan.

NIST Phase: Eradication

Reference: NIST 800-61r3 §3.4 — Eradication

Controls: NIST SI-2 (Flaw Remediation), NIST CM-3 (Configuration Change Control), CIS 7.3 (Perform Automated Operating System Patch Management), CIS 7.4 (Perform Automated Application Patch Management)

Compensating: Download the patched NetScaler firmware from the Citrix portal and verify the SHA-256 hash of the downloaded .tgz file against the hash published in CTX696300 before installation — do not skip hash verification on network appliance firmware. Apply via 'install build -Y' on each appliance CLI per the version-specific upgrade path in CTX696300. Post-install, confirm the build with 'show version' and verify the output matches the patched build number listed in CTX696300 for both CVE-2026-3055 and CVE-2026-4368. For teams without NetScaler Console Service, manually cross-reference the 'show version' output against the CTX696300 fixed version table as the verification step.

Evidence: Before patching, capture a full configuration backup via 'save ns config' and export /nsconfig/ns.conf as a pre-patch snapshot. Preserve the pre-patch 'show version' output as the baseline for change documentation. After patching, capture the post-patch 'show version' output and store both outputs together in the incident record to satisfy NIST CM-3 change control documentation requirements.

Step 4: Recovery — After patching, verify NetScaler ADC and Gateway services are operating normally. Re-run the NetScaler Console Service vulnerability assessment to confirm CVE-2026-3055 and CVE-2026-4368 are no longer flagged. Monitor application delivery and authentication logs for anomalies for at least 72 hours post-patch.

NIST Phase: Recovery

Reference: NIST 800-61r3 §3.5 — Recovery

Controls: NIST IR-4 (Incident Handling), NIST SI-6 (Security and Privacy Function Verification), NIST AU-6 (Audit Record Review, Analysis, and Reporting), CIS 7.2 (Establish and Maintain a Remediation Process)

Compensating: Verify Gateway and ADC virtual server health post-patch via 'show lb vserver' and 'show vpn vserver' — confirm all vservers show 'UP' state with no unexpected session drops. Monitor /var/nslog/ns.log continuously for 72 hours for any recurrence of crash or memory fault indicators: tail -f /var/nslog/ns.log | grep -iE 'segfault|core dump|error|fault'. For authentication log monitoring on Gateway, parse /var/nslog/ns.log for failed or anomalous EPA/VPN authentication events that could indicate post-patch exploitation attempts or residual access from pre-patch credential exposure.

Evidence: Capture 'show ns info' and 'show version' immediately post-patch and at 24/48/72-hour intervals as timestamped recovery verification records. Preserve /var/nslog/ns.log snapshots at each interval to create a post-patch baseline showing absence of memory fault events. If any memory leakage was suspected pre-patch, retain all pre-patch response captures alongside post-patch captures to demonstrate remediation.

Step 5: Post-Incident — Evaluate patch cadence for network edge appliances; Citrix NetScaler has had recurring critical CVEs. Confirm that NetScaler management interfaces are not internet-exposed. Document this patching event in your vulnerability management record and review whether automated advisory alerting

for Citrix products is in place.

NIST Phase: Post Incident

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

Controls: NIST IR-4 (Incident Handling), NIST IR-8 (Incident Response Plan), NIST SI-5 (Security Alerts, Advisories, and Directives), CIS 7.1 (Establish and Maintain a Vulnerability Management Process), CIS 4.4 (Implement and Manage a Firewall on Servers)

Compensating: Subscribe to the Citrix Security Advisory RSS feed (https://support.citrix.com/user/login — verify access) and CISA KEV feed (https://www.cisa.gov/known-exploited-vulnerabilities-catalog) for automated notification of new Citrix NetScaler CVEs without requiring enterprise tooling. Run 'show ns ip' and document that all NSIPs are bound to RFC 1918 addresses and verify no NSIP is reachable from internet-facing segments by running a firewall policy review or an nmap scan from an external vantage point: nmap -p 22,80,443,3010 from a DMZ-equivalent host. Document the full patching event — affected versions identified, patch applied, verification steps completed, and responsible staff — in your vulnerability management record to satisfy NIST IR-5 (Incident Monitoring) tracking requirements.

Evidence: Retain the complete pre-patch and post-patch 'show version' outputs, the ACL configuration captures from Step 1, and the detection log samples from Step 2 as the evidentiary record for this patching event. Archive the CTX696300 bulletin PDF alongside the incident record, as Citrix advisories have historically been revised or superseded; the version consulted at time of action should be preserved. Document the NSIP exposure assessment results (internal-only confirmation) as a control effectiveness record.

Detection Guidance

No confirmed IOCs or active exploitation indicators were present in the source data for CVE-2026-3055 at time of item generation. Detection focus should be on vulnerability presence rather than active compromise indicators. Use NetScaler Console Service instance advisory to scan for vulnerable firmware versions across managed appliances. In your SIEM, alert on NetScaler process fault or crash events (check NetScaler ns.log and newnslog for memory-related error codes). If network inspection is available, monitor for malformed or unexpectedly large responses from NetScaler Gateway or ADC virtual servers, which may indicate memory disclosure. Verify management plane access logs for unauthorized or anomalous administrative sessions coinciding with the public disclosure date of March 23, 2026.

Framework Mappings

ISO-27001-2022

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

Sources

Source	URL	Tier
	https://arcticwolf.com/resources/blog/cve-2026-3055/	T3
Citrix Security Bulletin for CVE-2026-3055 and CVE-2026-4368	https://support.citrix.com/support-home/kbsearch/article?articleNum...	T3

Source	URL	Tier
CVE-2026-3055: Citrix NetScaler ADC and NetScaler Gateway Out ...	https://www.rapid7.com/blog/post/etr-cve-2026-3055-citrix-netscaler...	T3
Identify and remediate vulnerabilities for CVE-2026-3055	https://docs.netscaler.com/en-us/netscaler-console-service/instance...	T3
CVE-2026-3055 - NVD	https://nvd.nist.gov/vuln/detail/CVE-2026-3055	T1

DISCLAIMER

This intelligence report is produced by Tech Jacks Solutions Security Command Center (SCC) for informational purposes only. It does not constitute professional security advice, legal counsel, or an incident response engagement. The information herein is derived from publicly available sources and AI-assisted analysis; while every effort is made to ensure accuracy, Tech Jacks Solutions makes no warranties regarding completeness or timeliness. Organizations should conduct their own validation and consult qualified security professionals before taking action based on this report. Tech Jacks Solutions is not liable for any damages resulting from the use of this information.

Generated 2026-03-29 18:44 UTC by TJS Security Command Center