Hive Pro

Threat Level

Red

Hiveforce Labs

THREAT ADVISORY

VULNERABILITY REPORT

CVE-2026-3055: Silent Memory Leak in NetScaler Actively Exploited

Date of Publication	Admiralty Code	TA Number
April 1, 2026	A1	TA2026087

Summary

First Seen: March 23, 2026
Affected Products: Citrix NetScaler ADC, Citrix NetScaler Gateway
Impact: Citrix NetScaler is actively being exploited to exploit CVE-2026-3055, a critical SAML flaw that enables attackers to leak sensitive memory data via crafted requests without authentication. The issue can expose session tokens and other confidential information, making it highly dangerous for internet-facing systems. Additionally, CVE-2026-4368 introduces a session mix-up risk that could enable session hijacking in specific configurations. With exploitation already observed in the wild, organizations should urgently apply patches and review their deployments.

CVEs

CVE	NAME	AFFECTED PRODUCT	ZERO-DAY	CISA KEV	PATCH
CVE-2026-3055	Citrix NetScaler Out-of-Bounds Read Vulnerability	Citrix NetScaler ADC and NetScaler Gateway	✗	✓	✓
CVE-2026-4368	Citrix NetScaler Race Condition Vulnerability		✗	✗	✓

Vulnerability Details

#1

Citrix has released fixes for a critical vulnerability affecting NetScaler ADC and NetScaler Gateway (CVE-2026-3055), an out-of-bounds memory read issue (CWE-125) within the SAML authentication processing logic. The flaw originates from a custom XML parsing implementation written in C, where improper input validation allows specially crafted SAML or WS-Federation requests to bypass integrity checks. When key attributes, such as AssertionConsumerServiceURL, are missing from authentication requests sent to endpoints, the appliance fails to validate their presence before accessing memory.

#2

Instead of rejecting these malformed requests, the system reads from uninitialized or previously freed memory and returns the exposed data to the requester, encoded within a Base64 NSC_TASS cookie. This behavior significantly increases the risk of sensitive information leakage from process memory.

#3

The vulnerability impacts NetScaler ADC and Gateway versions 14.1 before 14.1-66.59 and 13.1 before 13.1-62.23, including FIPS and NDcPP builds. Exploitation is limited to appliances configured as SAML Identity Providers, but the risk remains substantial due to the flaw's network accessibility, low complexity, and lack of authentication requirements, reflected in its CVSS 4.0 score of 9.3. Reports have already confirmed in-the-wild exploitation shortly after disclosure, reinforcing the need for immediate patching.

#4

Alongside this, Citrix also addressed CVE-2026-4368, a race condition vulnerability (CWE-362) affecting session handling in specific NetScaler Gateway and AAA configurations. This flaw can lead to session mix-ups, potentially allowing one user to access another's session data. While its impact is limited to version 14.1-66.54 and requires partial authentication, it still poses a meaningful risk in multi-user environments.

#5

Together, these issues highlight systemic gaps in input validation and concurrent session handling, underscoring the importance of promptly applying updates and auditing authentication configurations to prevent exposure. Anyone using affected versions must apply the necessary patches urgently.

Vulnerabilities

CVE ID	AFFECTED PRODUCTS	AFFECTED CPE	CWE ID
CVE-2026-3055	NetScaler ADC and NetScaler Gateway 14.1 BEFORE 14.1-60.58 NetScaler ADC and NetScaler Gateway 13.1 BEFORE 13.1-62.23 NetScaler ADC FIPS and NDcPP BEFORE 13.1-37.262	cpe:2.3:a:citrix:netscaler_application_delivery_controller:*:*:*:*:fips:*:*:* cpe:2.3:a:citrix:netscaler_application_delivery_controller:*:*:*:*:ndcpp:*:*:* cpe:2.3:a:citrix:netscaler_application_delivery_controller:*:*:*:*:-:*:*:* cpe:2.3:a:citrix:netscaler_gateway:*:*:*:*:*:*:*:*	CWE-125
CVE-2026-4368	NetScaler ADC and NetScaler Gateway 14.1-66.54	cpe:2.3:a:citrix:netscaler_adc:*:*:*:*:*:*:*:* cpe:2.3:a:citrix:netscaler_gateway:*:*:*:*:*:*:*:*	CWE-362

Recommendations

Apply Vendor Patches Immediately: Upgrade all affected NetScaler ADC and NetScaler Gateway appliances to the latest patched versions without delay. The fixed versions are 14.1-66.59 and later for the 14.1 branch, 13.1-62.23 and later for the 13.1 branch, and 13.1-37.262 and later for 13.1-FIPS and 13.1-NDcPP builds. Given confirmed active exploitation of CVE-2026-3055, this should be treated as an emergency patching activity with the highest priority. Organizations on build 14.1-66.54 should upgrade immediately to also address CVE-2026-4368.

Verify Configuration Exposure for Both CVEs: **For CVE-2026-3055, inspect the NetScaler configuration for add authentication samlIdPProfile to determine SAML IDP exposure. For CVE-2026-4368, check for add authentication vserver (AAA) or add vpn vserver (Gateway). Note that CVE-2026-4368 only affects build 14.1-66.54, organizations on other versions are not exposed to the race condition but remain in scope for CVE-2026-3055 if running affected versions.**

Inspect Logs for Indicators of Exploitation: Review `/var/log/ns.log` on affected appliances for anomalous SAML-related error messages, particularly entries referencing unexpected or empty `ProtocolBinding` or `ACSURL` values. Unusual patterns of POST requests to `/saml/login` or GET requests to `/wsfed/passive?wctx` with missing parameter values should be investigated as potential exploitation attempts.

Rotate Sessions and Credentials Post-Patching: After applying the patches, invalidate all active user and administrative sessions on the appliance. If exploitation cannot be ruled out, rotate all credentials that may have been exposed through the appliance, including administrative passwords and any session tokens for downstream applications that were processed through the NetScaler.

Vulnerability Management: Establish a continuous vulnerability management process that prioritizes the timely assessment and remediation of critical vulnerabilities in internet-facing appliances. Maintain an accurate inventory of all NetScaler appliance versions and configurations, subscribe to Citrix security bulletins for timely notification of future advisories, and evaluate the ongoing security posture of third-party network appliances as part of your organization's risk management framework.

Potential MITRE ATT&CK TTPs

Tactic	Technique	Sub-technique
Initial Access	T1190: Exploit Public-Facing Application	
Credential Access	T1212: Exploitation for Credential Access	
	T1539: Steal Web Session Cookie	
Collection	T1005: Data from Local System	
Lateral Movement	T1563: Remote Service Session Hijacking	
Resource Development	T1588: Obtain Capabilities	T1588.006: Vulnerabilities

Patch Link

https://support.citrix.com/support-home/kbsearch/article?articleNumber=CTX696300

References

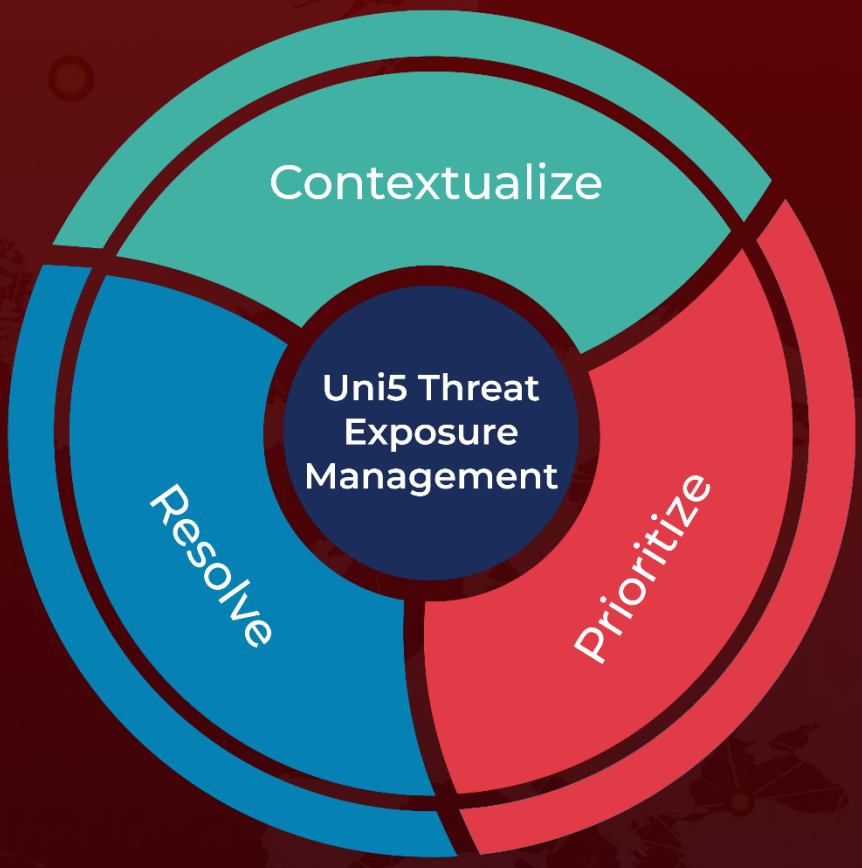
https://labs.watchtowr.com/the-sequels-are-never-as-good-but-were-still-in-pain-citrix-netscaler-cve-2026-3055-memory-overread/

https://labs.watchtowr.com/please-we-beg-just-one-weekend-free-of-appliances-citrix-netscaler-cve-2026-3055-memory-overread-part-2/

What Next?

At **Hive Pro**, it is our mission to detect the most likely threats to your organization and to help you prevent them from happening.

Book a free demo with **HivePro Uni5**: Threat Exposure Management Platform.



REPORT GENERATED ON

April 01, 2026 • 08:40 AM

More at www.hivepro.com