

HiveForce Labs

THREAT ADVISORY

 VULNERABILITY REPORT

Critical NetScaler SAML Flaw Opens Path to Remote Code Execution

Date of Publication

October 12, 2026

Admiralty Code

A1

TA Number

TA2026297

Summary

First Seen: October 8, 2026

Affected Products: Citrix NetScaler ADC, Citrix NetScaler Gateway

Impact: CVE-2026-107406 is a critical memory overflow vulnerability (CWE-119, CVSS v4.0 9.5) in customer-managed Citrix NetScaler ADC and NetScaler Gateway appliances that allows unauthenticated remote attackers to achieve code execution or crash the device. Exploitation requires the appliance to be configured as a SAML Identity Provider or Service Provider, and the flaw affects the 14.1 and 13.1 release lines, their FIPS and NDcPP builds, and Secure Private Access Hybrid deployments. No in-the-wild exploitation has been reported; however, given how quickly earlier NetScaler flaws were weaponized this year, organizations should upgrade to the patched builds immediately.

CVE

CVE	NAME	AFFECTED PRODUCT	ZERO-DAY	CISA KEV	PATCH
CVE-2026-107406	Citrix NetScaler ADC and NetScaler Gateway Memory Overflow Vulnerability	Citrix NetScaler ADC and NetScaler Gateway			

Vulnerability Details

#1

Citrix NetScaler ADC and NetScaler Gateway are application delivery and secure remote access appliances that typically sit at the network perimeter and broker authentication for enterprise applications. CVE-2026-107406 is a critical memory overflow vulnerability in these appliances, classified as CWE-119 (Improper Restriction of Operations within the Bounds of a Memory Buffer), that can result in remote code execution or a denial-of-service condition that crashes the device.

#2

Exposure depends on SAML configuration and build. On NetScaler ADC and Gateway releases earlier than 14.1-73.37 and 13.1-64.23, and the corresponding 14.1-FIPS and 13.1-FIPS/NDcPP builds, appliances configured as either a SAML SP or SAML IdP are vulnerable. On builds 14.1-73.37 through 14.1-73.41 (including 14.1-FIPS), 13.1-64.23 through 13.1-64.28, and 13.1-FIPS/NDcPP 13.1-37.279 through 13.1-37.282, only SAML IdP configurations are affected. Secure Private Access Hybrid deployments using NetScaler instances are also in scope, while Citrix-managed cloud services and Adaptive Authentication are updated by the vendor.

#3

The flaw carries a CVSS v4.0 base score of 9.5, reflecting network-based exploitation that requires no privileges or user interaction, tempered by high attack complexity, with high confidentiality, integrity, and availability impact on the appliance and high confidentiality and integrity impact on subsequent systems. The vendor has not disclosed the vulnerable code path, and no in-the-wild exploitation was known at disclosure.

#4

The risk is amplified by NetScaler's 2026 exploitation record. Flaws patched in March came under attack within days, [CVE-2026-88771](#) and [CVE-2026-88772](#) were exploited as zero-days in September to deploy web shells and tunneling malware, steal credentials, and gain root access, and [CVE-2026-88779](#), which shares the same SAML precondition, was added to KEV in October. CISA has included CVE-2026-107406 in its NetScaler alert, and internet scans count over 21,000 exposed instances.

Vulnerability

CVE ID	AFFECTED PRODUCTS	AFFECTED CPE	CWE ID
CVE-2026-107406	Citrix NetScaler ADC and NetScaler Gateway (14.1-73.41 and earlier, 13.1-64.28 and earlier), Citrix NetScaler ADC 14.1-FIPS (14.1-73.41 FIPS and earlier), Citrix NetScaler ADC 13.1-FIPS and 13.1-NDcPP (13.1-37.282 and earlier)	cpe:2.3:a:citrix:netscaler_application_delivery_controller:*:*:*:*:*:*:**, cpe:2.3:a:citrix:netscaler_gateway:*:*:*:*:*:*:*	CWE-119

Recommendations



Upgrade to Fixed Releases Immediately: Upgrade affected appliances to NetScaler ADC and NetScaler Gateway 14.1-73.46 or later, 13.1-64.29 or later releases of 13.1, NetScaler ADC 14.1-FIPS 14.1-73.46 FIPS or later, and NetScaler ADC 13.1-FIPS and 13.1-NDcPP 13.1-37.283 or later. Prioritize internet-facing appliances configured as a SAML IdP or SP, and treat the upgrade as an emergency change given how quickly earlier NetScaler flaws were weaponized this year. Confirm that the earlier fixes for CVE-2026-88771 through CVE-2026-88779 are also in place on every appliance.



Confirm SAML Exposure on Every Appliance: Review the configuration of each NetScaler instance for "add authentication samlAction", which indicates a SAML SP, and "add authentication samlIdPProfile", which indicates a SAML IdP. Map the result against the installed build, since appliances on 14.1-73.37 to 14.1-73.41 or 13.1-64.23 to 13.1-64.28 are exposed only as an IdP, whereas older builds are exposed in either role.



Include Secure Private Access Hybrid Instances: Extend patching to NetScaler instances that support Secure Private Access Hybrid deployments, which are confirmed as affected. Citrix-managed cloud services and Adaptive Authentication are upgraded by the vendor, but every customer-managed NetScaler instance in the access path remains the organization's responsibility.



Reduce Exposure Until Patching Completes: No workaround has been published, so upgrading is the only complete fix. Where a SAML IdP or SP profile is not operationally required, removing it eliminates the exploitation precondition; where SAML authentication must remain enabled, place the affected appliances under heightened monitoring until the upgrade is complete.



Check for Compromise Before Patching: Assess appliances for signs of compromise before applying updates, using the indicators of compromise Citrix provides through NetScaler Console and CISA's SIGMA detection rule, and review appliances for unfamiliar files, accounts, and outbound connections given the web shells and tunneling malware seen in earlier NetScaler intrusions this year. Treat unexpected crashes or reboots as suspicious, and forward NetScaler logs to a SIEM or central log store, since local logs rotate quickly and can overwrite forensic artifacts.



Preserve Evidence and Restore Trust After Suspected Compromise: If compromise is suspected, preserve forensic evidence before updating, since updates can reduce forensic visibility, then restore a known-good backup that predates the suspected compromise and rotate all restored secrets, including local account passwords, key-encryption keys, and SSL certificates. For appliances acting as a SAML IdP or SP, also rotate SAML signing certificates and invalidate active federated sessions so stolen material cannot be reused.



Strengthen Edge Device Vulnerability Management: Maintain an accurate inventory of NetScaler and other perimeter appliances, including build numbers and enabled authentication features, and define an emergency patch window for critical edge-device flaws. Subscribe to Citrix security bulletin alerts so new advisories reach the responsible team on the day of publication.



Potential MITRE ATT&CK TTPs

Tactic	Technique	Sub-technique
Initial Access	<u>T1190</u> : Exploit Public-Facing Application	
Impact	<u>T1499</u> : Endpoint Denial of Service	<u>T1499.004</u> : Application or System Exploitation



Patch Link

<https://support.citrix.com/external/article/CTX697191/citrix-netScaler-adc-and-citrix-netscale.html>



References

<https://support.citrix.com/external/article/CTX697191/citrix-netScaler-adc-and-citrix-netscale.html>

<https://www.cisa.gov/news-events/alerts/2026/09/27/critical-zero-day-vulnerabilities-exploited-citrix-netScaler-adc-gateway>

https://community.citrix.com/techzone-blogs/110_security-updates/protecting-customers-immediate-guidance-for-cve-2026-107406-in-netScaler-adc-and-netScaler-gateway-r1631/

<https://www.hivepro.com/threat-advisory/citrix-netScaler-zero-days-under-active-exploitation>

<https://www.hivepro.com/threat-advisory/citrix-netScaler-saml-zero-day-cve-2026-88779-under-active-exploitation>



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 Demo of HivePro.

REPORT GENERATED ON

October 12, 2026 • 11:30 PM

© 2026 All Rights are Reserved by Hive Pro



More at www.hivepro.com