

HiveForce Labs

THREAT ADVISORY

 VULNERABILITY REPORT

Citrix NetScaler SAML Zero-Day CVE-2026-88779 Under Active Exploitation

Date of Publication

October 6, 2026

Admiralty Code

A1

TA Number

TA2026290

Summary

First Seen: October 1, 2026

Affected Products: Citrix NetScaler ADC, Citrix NetScaler Gateway, Citrix NetScaler ADC FIPS, Citrix NetScaler ADC NDcPP

Impact: CVE-2026-88779 is a high-severity memory overflow zero-day in Citrix NetScaler ADC and NetScaler Gateway, and it is being actively exploited against appliances configured as a SAML Service Provider or Identity Provider. Attackers hide shell commands in the username field of crafted SAML authentication requests, which repeatedly crash and reboot the appliance and allow them to download and run a payload that plants web shells, persists across reboots, and steals the appliance configuration and backups.

CVE

CVE	NAME	AFFECTED PRODUCT	ZER O-DAY	CISA KEV	PATC H
CVE-2026-88779	Citrix NetScaler Improper Restriction of Operations within the Bounds of a Memory Buffer Vulnerability	Citrix NetScaler ADC, Citrix NetScaler Gateway			

Vulnerability Details

#1

Citrix has released emergency security updates for CVE-2026-88779, a high-severity memory overflow vulnerability in Citrix NetScaler ADC and NetScaler Gateway that has been exploited in the wild as a zero-day. The flaw affects only appliances configured as a SAML Service Provider (SP) or SAML Identity Provider (IdP). Affected products are NetScaler ADC and NetScaler Gateway, NetScaler ADC FIPS before 14.1-73.41 FIPS, and NetScaler ADC FIPS and NDcPP before 13.1-37.282. Secure Private Access hybrid deployments are also affected. Citrix has observed targeted attacks on unmitigated deployments, and exploitation also hit appliances patched only days earlier for [CVE-2026-88771 and CVE-2026-88772](#). No threat actor or named malware family has been linked to the activity. CISA has added CVE-2026-88779 to its Known Exploited Vulnerabilities (KEV) catalog and directed federal agencies to remediate by October 7, 2026.

#2

The vulnerability is classified as Improper Restriction of Operations within the Bounds of a Memory Buffer and resides in the appliance's SAML authentication handling. The vulnerable code is reachable only when the appliance is configured as a SAML SP through the add authentication samlAction command or as a SAML IdP through the add authentication samlIdPProfile command. Exposure therefore depends on configuration, but it sits directly on the internet-facing authentication surface.

#3

Attackers exploit the flaw remotely, without authentication or user interaction, by sending crafted SAML authentication requests that embed shell commands in the username field to download and execute a payload. These requests crash the nsaaad process repeatedly until the NetScaler Pitboss process reaches its restart limit and reboots the appliance. This explains the unexpected reboots reported by administrators, including on systems running 14.1-73.37. A downloaded binary was observed running on at least one honeypot, where it attempts to plant web shells, survive reboots, and upload the appliance configuration and backups. These behaviors point to code execution and data theft well beyond the denial-of-service impact stated by Citrix.

#4

Repeated crashes take down remote access, SAML single sign-on, and application delivery for every user who depends on the affected appliance. Because NetScaler sits at the network edge and handles authentication for VPN, virtual desktop, and federated web applications, an outage directly disrupts workforce productivity and customer-facing services. Citrix states it has not identified any impact on customer data integrity, but the observed web shells, persistence, and configuration theft suggest the real risk extends to full appliance compromise and exposure of stored credentials, certificates, and keys. With active exploitation, the KEV listing, and a three-day federal deadline, this vulnerability should be a top remediation priority for any organization running SAML-enabled NetScaler appliances.

Vulnerability

CVE ID	AFFECTED PRODUCTS	AFFECTED CPE	CWE ID
CVE-2026-88779	Citrix NetScaler ADC and NetScaler Gateway 14.1 (Before 14.1-73.41), Citrix NetScaler ADC and NetScaler Gateway 13.1 (Before 13.1-64.28), Citrix NetScaler ADC 14.1-FIPS (Before 14.1-73.41 FIPS), Citrix NetScaler ADC 13.1-FIPS and 13.1-NDcPP (Before 13.1-37.282)	cpe:2.3:a:citrix:netscaler_application_delivery_controller:*:*:*:*:*:*:*:* cpe:2.3:a:citrix:netscaler_gateway:*:*:*:*:*:*:*:* cpe:2.3:a:citrix:netscaler_application_delivery_controller:*:*:*:*:*:*:*:*:fips:*:*:* cpe:2.3:a:citrix:netscaler_application_delivery_controller:*:*:*:*:*:*:*:*:ndcpp:*:*:*	CWE-119

Recommendations



Upgrade to Fixed Builds Immediately: Upgrade every NetScaler ADC and NetScaler Gateway appliance to 14.1-73.41, 13.1-64.28, 14.1-73.41 FIPS, or 13.1-37.282 and later releases as published in Citrix bulletin CTX697174. Prioritize internet-facing appliances that broker SAML authentication, and do not rely on the previous patch cycle, since exploitation has already hit appliances that were patched only days earlier for CVE-2026-88771 and CVE-2026-88772.



Confirm Whether SAML Is Configured: Review the running configuration of every appliance for the add authentication samlAction and add authentication samIIdPProfile entries, which mark an appliance as a SAML Service Provider or SAML Identity Provider and therefore vulnerable. Maintain this list as the priority scope for patching, hunting, and monitoring, and include Secure Private Access hybrid deployments in the review.



Apply the Citrix Global Deny List: Enable the Citrix-released Global Deny List to block known malicious IP addresses associated with this activity, and add 213[.]209[.]159[.]55 to the perimeter firewall, proxy, and appliance deny lists. Treat these blocks as a temporary control that reduces exposure while upgrades are scheduled, not as a substitute for patching.



Treat Exploited Appliances as Compromised: If any indicator of exploitation is found, isolate the appliance, preserve forensic artifacts, and rebuild it from a known-good image before returning it to service, since the observed payload attempts to persist across reboots. Because the payload attempts to upload configuration and backups, rotate all credentials, service account secrets, SAML signing material, TLS certificates, and keys stored on or used by the appliance.



Monitor Authentication Logs for Anomalous Usernames: Inspect SAML and AAA authentication logs for usernames containing shell metacharacters, command strings, or embedded IP addresses, which match the exploitation pattern described in public reporting. Forward NetScaler logs to a central SIEM and create alerts for nsaaad process crashes, appliance reboots, and authentication requests with malformed username values.



Potential MITRE ATT&CK TTPs

Tactic	Technique	Sub-technique
Initial Access	<u>T1190</u> : Exploit Public-Facing Application	
Execution	<u>T1059</u> : Command and Scripting Interpreter	<u>T1059.004</u> : Unix Shell
Command and Control	<u>T1105</u> : Ingress Tool Transfer	
Persistence	<u>T1505</u> : Server Software Component	<u>T1505.003</u> : Web Shell
Collection	<u>T1005</u> : Data from Local System	
Exfiltration	<u>T1041</u> : Exfiltration Over C2 Channel	
Impact	<u>T1499</u> : Endpoint Denial of Service	<u>T1499.004</u> : Application or System Exploitation



Indicators of Compromise (IOCs)

TYPE	VALUE
IPv4	213[.]209[.]159[.]55
File Path	/v





Patch Link

<https://support.citrix.com/external/article/CTX697174/citrix-netscaler-adc-and-citrix-netscale.html>



References

https://community.citrix.com/techzone-blogs/110_security-updates/understanding-and-addressing-cve-2026-88779-in-citrix-netscaler-adc-and-citrix-netscaler-gateway/

<https://support.citrix.com/external/article/CTX697174/citrix-netscaler-adc-and-citrix-netscale.html>

https://www.hkcert.org/security-bulletin/citrix-products-denial-of-service-vulnerability_20261005

<https://www.hivepro.com/threat-advisory/citrix-netscaler-zero-days-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 06, 2026 • 3:30 AM

© 2026 All Rights are Reserved by Hive Pro



More at www.hivepro.com