

HiveForce Labs

THREAT ADVISORY

 VULNERABILITY REPORT

Citrix NetScaler Zero-Days Under Active Exploitation

Date of Publication

September 28, 2026

Admiralty Code

A1

TA Number

TA2026285

Summary

First Seen: September 26, 2026

Affected Products: Citrix NetScaler ADC and Citrix NetScaler Gateway

Impact: Citrix has confirmed two critical remote code execution vulnerabilities, CVE-2026-88771 and CVE-2026-88772, in its NetScaler ADC and NetScaler Gateway appliances, both exploited in the wild as zero-days before any fix was available. CVE-2026-88771 comes from improper input validation and lets an unauthenticated attacker run arbitrary commands on the appliance, affecting every deployment on an affected version, including the default configuration. CVE-2026-88772 is a memory overflow that can lead to code execution or a denial-of-service condition when DTLS is enabled, which is the default state for VPN virtual servers. Because NetScaler devices sit at the network edge and handle VPN, remote access, load balancing, and user authentication, a compromised appliance hands an attacker a foothold at the perimeter and a path toward internal systems. Citrix published security bulletin CTX697096 with fixed builds on September 27, 2026. No threat actor or malware family has been publicly attributed.

⚙ CVEs

CVE	NAME	AFFECTED PRODUCT	ZER O-DAY	CISA KEV	PATC H
CVE-2026-88771	Citrix NetScaler Improper Input Validation Vulnerability	Citrix NetScaler ADC / NetScaler Gateway	✔	✔	✔
CVE-2026-88772	Citrix NetScaler Improper Restriction of Operations within the Bounds of a Memory Buffer Vulnerability	Citrix NetScaler ADC / NetScaler Gateway	✔	✔	✔

Vulnerability Details

#1

Both CVE-2026-88771 and CVE-2026-88772 are critical remote code execution vulnerabilities in Citrix NetScaler ADC and NetScaler Gateway that attackers exploited in the wild before a fix was available. CVE-2026-88771 is an improper input validation flaw (CWE-20). The appliance fails to properly check attacker-supplied input, which allows an unauthenticated user to inject and execute arbitrary operating-system commands on the device. It affects all NetScaler ADC and NetScaler Gateway deployments running an affected build, including those left in the default configuration, and no optional feature needs to be enabled for it to work.

#2

CVE-2026-88772 is a memory overflow vulnerability, a memory-corruption weakness in the CWE-119 family. By overrunning a memory buffer on the appliance, an attacker can either execute code remotely or crash the service, producing a denial-of-service condition. The precondition is that DTLS is enabled, which is the default for VPN virtual servers, so most NetScaler Gateway deployments meet it unless DTLS has been deliberately turned off. A pre-disclosure notice attributed to the Dutch NCSC described one of the flaws as letting an attacker place shellcode directly into memory, consistent with this memory-overflow behavior.

#3

Both vulnerabilities are exploitable over the network against the appliance's public-facing interfaces with no authentication required, which is what makes internet-exposed NetScaler Gateway, VPN, and AAA virtual servers the highest-priority targets. The affected releases are 14.1 before 14.1-73.37, 13.1 before 13.1-64.23, 14.1-FIPS before 14.1-73.37 FIPS, and 13.1-FIPS and 13.1-NDcPP before 13.1-37.279. Secure Private Access hybrid deployments that rely on NetScaler instances are also affected. The bulletin covers customer-managed appliances; Citrix updates its own managed cloud services separately.

#4

Both flaws are rated 9.5 (Critical) under CVSS 4.0. Citrix confirmed that exploits of CVE-2026-88771 and CVE-2026-88772 have been observed against unmitigated NetScaler deployments and said it discovered the vulnerabilities while investigating incidents in customer environments. Citrix has not published a workaround, so upgrading to a fixed build is the only remediation. With active exploitation confirmed and no workaround available, patching is urgent: organizations should update every affected NetScaler ADC and NetScaler Gateway appliance to a fixed build immediately and prioritize any that are internet-facing.

Vulnerabilities

CVE ID	AFFECTED PRODUCTS	AFFECTED CPE	CWE ID
CVE-2026-88771	Citrix NetScaler ADC & NetScaler Gateway (14.1 before 14.1-73.37; 13.1 before 13.1-64.23; 14.1-FIPS before 14.1-73.37 FIPS; 13.1-FIPS & 13.1-NDcPP before 13.1-37.279)	cpe:2.3:a:citrix:netscaler_application_delivery_controller:*:*:*:*:*:* *, cpe:2.3:a:citrix:netscaler_gateway:*:*:*:*:*:* :*	CWE-20
CVE-2026-88772	Citrix NetScaler ADC & NetScaler Gateway (ADC: before 14.1-73.37, before 13.1-64.23, before 14.1-73.37 FIPS, and before 13.1.37.279 FIPS and NDcPP; Gateway: before 14.1-73.37 and before 13.1-64.23)	cpe:2.3:a:citrix:netscaler_application_delivery_controller:*:*:*:*:*:* *, cpe:2.3:a:citrix:netscaler_gateway:*:*:*:*:*:* :*	CWE-119

Recommendations



Preserve Forensic Evidence First: Before making any changes, capture the logs, a system snapshot, a technical support bundle, and a core dump from every exposed appliance. Because the attacks happened before a fix existed, patching can overwrite the very traces that would show whether you were breached, so collecting evidence up front is essential for any later investigation.



Update to the Fixed Builds Without Delay: Upgrade every NetScaler ADC and NetScaler Gateway to the fixed build for its branch (14.1-73.37, 13.1-64.23, 14.1-73.37 FIPS, or 13.1-37.279), and update Secure Private Access hybrid deployments to the recommended builds. There is no workaround, so upgrading is the only fix. On 13.1, run `show ns variable` first; if it returns any variables, use 13.1-64.24 to avoid a known reboot loop during the upgrade.



Assume Compromise and Hunt for It: Run the IOC scan available on the NetScaler Console Security Advisory page, or request the indicators from Citrix Support, and consider the Dutch NCSC check scripts as an additional pass. Treat any internet-facing appliance as potentially compromised until proven otherwise, and remember that a clean scan is not proof of safety, because the published indicators do not cover every technique.



Rotate Credentials, Secrets, and Certificates: Reset the passwords of every service account and user that authenticated through the appliance, replace any secrets stored on it, and revoke and reissue its certificates and private keys. A compromised NetScaler can expose everything it holds or brokers, so rotating credentials limits what an attacker can reuse after you patch.



Reduce Internet Exposure of the Management Plane: Keep NetScaler management interfaces off the public internet, and where you cannot patch immediately, isolate or limit the exposure of affected appliances until you can. Forward NetScaler logs to your SIEM so that exploitation attempts and post-exploitation activity are captured centrally.



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	
Impact	<u>T1499</u> : Endpoint Denial of Service	
Resource Development	<u>T1588</u> : Obtain Capabilities	<u>T1588.006</u> : Vulnerabilities



Patch Link

<https://support.citrix.com/support-home/kbsearch/article?articleNumber=CTX697096>



References

<https://support.citrix.com/support-home/kbsearch/article?articleNumber=CTX697096>

<https://watchtower.com/intelligence/citrix-netscaler-adc-citrix-netscaler-gateway-remote-code-execution-cve-2026-88771/>



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

September 28, 2026 • 07:45 AM

© 2026 All Rights are Reserved by Hive Pro



More at www.hivepro.com