Critical Citrix NetScaler Vulnerabilities Allow Authentication Bypass and Denial of Service

Author: *Portia S. Cole – CTI Researcher*

TL;DR

Two vulnerabilities affect Citrix NetScaler ADC and NetScaler Gateway. CVE-2026-19490 (CVSS 9.3) allows authentication bypass, while CVE-2026-19489 (CVSS 8.8) can cause a denial of service.

There is no evidence of active exploitation. Citrix urges customers to upgrade immediately because no workarounds are available.

Overview

There are two vulnerabilities in customer-managed Citrix NetScaler ADC and NetScaler Gateway appliances. CVE-2026-19490 (CVSS 9.3) can allow an unauthenticated remote attacker to bypass authentication. CVE-2026-19489 (CVSS 8.8) can cause the appliance to become unstable or unavailable.

NetScaler ADC distributes application traffic across servers, while NetScaler Gateway provides secure remote access to internal applications and services.

Vulnerability Breakdown

- **CVE-2026-19490** (CVSS 9.3, Critical): An authentication bypass vulnerability that can be exploited remotely without credentials or user interaction. The appliance must be configured as a Gateway, including SSL VPN, ICA Proxy, CVPN or RDP Proxy, or as an AAA virtual server. Newer builds are only affected when a SAML authentication action is also configured.

- **CVE-2026-19489** (CVSS 8.8, High): A memory overflow vulnerability that can cause unpredictable behavior or a denial of service. The flaw can be exploited remotely without authentication when SIP ALG is enabled on a Large Scale NAT group.

Affected Products

- NetScaler ADC and NetScaler Gateway 14.1 before 14.1-73.32
- NetScaler ADC and NetScaler Gateway 13.1 before 13.1-63.21
- NetScaler ADC FIPS 14.1 before 14.1-73.32 FIPS
- NetScaler ADC FIPS and NDcPP 13.1 before 13.1-37.277

Citrix urges customers to upgrade immediately because no workarounds are available. There is no public evidence of active exploitation. Citrix-managed cloud services have

Published on: 8/21/2026

already been updated, but Secure Private Access Hybrid deployments using customer-managed NetScaler instances are affected.

Impact on Aspire Customers

NetScaler appliances are commonly placed at the network edge. An attacker who exploits CVE-2026-19490 could bypass authentication and access applications or resources protected by the appliance. What the attacker could reach would depend on the customer's configuration. Exploitation of CVE-2026-19489 could disrupt remote access or prevent users from reaching applications delivered through NetScaler ADC.

The Common Vulnerability Scoring System (CVSS) rates vulnerabilities from 0 to 10 based on exploitability and potential impact.

- None (0.0): No severity
- Low (0.1–3.9): Limited impact
- Medium (4.0–6.9): Moderate risk
- High (7.0–8.9): Serious impact
- Critical (9.0–10.0): Severe impact requiring urgent attention

Aspire Protects

- **Patch** - CVE-2026-19490
  - Upgrade affected appliances to the appropriate fixed version.
  - Check for add authentication samlAction.*, add authentication vserver .* and add vpn vserver .* to determine whether the authentication bypass preconditions are present.
  - Prioritize internet-facing NetScaler Gateway and AAA virtual server deployments.
  - Review NetScaler authentication and Gateway logs for unexpected successful sessions or suspicious access.
- **Patch** - CVE-2026-19489
  - Upgrade affected appliances to the appropriate fixed version.
  - Check for add `lsn group.*sipalg.*` to determine whether SIP ALG is enabled on a Large Scale NAT group.
  - Review appliance logs for crashes, unexpected restarts or service interruptions.

TTPs to Watch

Initial Access

- Exploit Public-Facing Application [T1190]: An attacker may exploit the authentication bypass vulnerability on an internet-facing NetScaler Gateway or AAA virtual server. (CVE-2026-19490)

Impact

- Endpoint Denial of Service: Application or System Exploitation [T1499.004]: An attacker may exploit the memory overflow vulnerability to disrupt an affected NetScaler appliance. (CVE-2026-19489)

IoCs

There are no known IoCs at this time. Aspire is actively monitoring and will notify customers if any are found. For more details on how we can help protect your organization, contact Aspire's Customer Success Management team.

Targeted Industries

The vulnerabilities could affect organizations in any sector that use customer-managed NetScaler ADC or NetScaler Gateway appliances, including:

- Public Sector
- Energy
- Legal & Professional Services
- Healthcare
- Finance
- Education
- Retail
- Manufacturing

Aspire Service Offerings

- **Aspire Managed XDR (MXDR)**
  - Aspire Managed XDR (MXDR) combines next-generation eXtended Detection and Response (XDR) technology, a 24x7 security operations center (SOC), and the expertise of a US-based team of security professionals to identify and respond to threats across a broader attack surface.
  - Building on the existing capabilities of Managed Detection and Response (MDR), Aspire Managed XDR integrates and correlates telemetry from endpoints, network, cloud, email, identity, and more. This advanced

platform creates valuable context enabling end-to-end visibility across all threat vectors.
  - Experienced security analysts and incident responders deliver 24x7 threat detection, analysis, and investigations – with both automated and human-led response actions to quickly mitigate cyber attacks.

- **Aspire Incident Response**
  - The ability to respond effectively to data breaches is critical to every organization. When attacks occur, IT leaders need a process that will ultimately maintain business continuity, protect the company's reputation, and avoid fines, legal fees, and remediation costs.
  - Aspire offers incident response services to help you prepare for, manage, and recover from data breaches and network attacks. An experienced team uses industry-leading threat intelligence and the most current security technology to quickly respond to attacks, reduce damage, and minimize exposure.

- **NOC Services Notice**
  - If you are an Aspire NOC customer and are affected by these vulnerabilities, Aspire will open a case on your behalf. Customers interested in NOC services should contact Aspire's Customer Success Management team.

Supporting Documentation

CITRIX | Support
CITRIX | Support
NVD - CVE-2026-19489
NVD - CVE-2026-19490