

Critical Citrix NetScaler RCE Zero-Days Under Active Exploitation

Author: Portia S. Cole – CTI Researcher

Overview

Citrix released security updates for eight vulnerabilities affecting customer-managed NetScaler ADC and NetScaler Gateway appliances. Two (CVE-2026-88771 and CVE-2026-88772) were exploited as zero-days before patches became available.

NetScaler appliances are commonly used for VPN access, authentication, load balancing, and access to internal applications. Since these systems often face the internet, an attacker who takes control of one may be able to reach resources behind it.

CVE-2026-88771 affects every vulnerable NetScaler ADC and NetScaler Gateway deployment, including systems using the default configuration. CVE-2026-88772 applies when Datagram Transport Layer Security (DTLS) is enabled. DTLS is enabled by default on VPN virtual servers.

Citrix has not released details about the attacks or the groups behind them.

Vulnerability Breakdown

CVE-2026-88771 (CVSS 9.5)

- Improper input validation allows an unauthenticated attacker to send a malicious request and run commands on the appliance. The flaw affects all vulnerable NetScaler ADC and NetScaler Gateway deployments. No additional feature or configuration change is required.

CVE-2026-88772 (CVSS 9.5)

- A memory overflow can allow remote code execution or cause the appliance to stop responding. The vulnerability affects NetScaler systems with DTLS enabled, including VPN virtual servers where DTLS has not been explicitly disabled.

TL;DR

There are two critical vulnerabilities (CVE-2026-88771, CVSS 9.5 and CVE-2026-88772, CVSS 9.5) in Citrix NetScaler ADC and NetScaler Gateway.

Citrix confirmed that attackers are exploiting both vulnerabilities.

Successful exploitation could allow remote code execution on the appliance. One vulnerability can also cause a denial of service.

Affected Products

- Citrix NetScaler ADC and NetScaler Gateway 14.1 before 14.1-73.37
- Citrix NetScaler ADC and NetScaler Gateway 13.1 before 13.1-64.23
- Citrix NetScaler ADC 14.1-FIPS before 14.1-73.37 FIPS
- Citrix NetScaler ADC 13.1-FIPS before 13.1-37.279
- Citrix NetScaler ADC 13.1-NDcPP before 13.1-37.279
- Secure Private Access Hybrid deployments using affected NetScaler instances

The security advisory applies to customer-managed appliances. Citrix is updating its managed cloud services and managed Adaptive Authentication environments.

Other Vulnerabilities

Citrix fixed six additional NetScaler vulnerabilities in the same update. Active exploitation has not been reported for these flaws.

- **CVE-2026-88773** (CVSS 9.3) - HTTP request smuggling affecting systems with HTTP or SSL virtual servers.
- **CVE-2026-88774** (CVSS 7.0) - A policy bypass involving HTTP URL-based expressions.
- **CVE-2026-88775** (CVSS 8.8) - A memory overflow affecting Gateway and AAA virtual server configurations.
- **CVE-2026-88776** (CVSS 8.8) - A memory overflow affecting Oracle load-balancing virtual servers.
- **CVE-2026-88777** (CVSS 8.8) - A memory overflow affecting certain load-balancing, content-switching, CGNAT, LSN, and NAT64 configurations.
- **CVE-2026-88778** (CVSS 8.8) - Predictable TCP initial sequence numbers that may allow traffic interception or connection manipulation under certain conditions.

Impact on Aspire Customers

Someone exploiting either flaw could run commands on the NetScaler appliance without logging in. If the device controls VPN or application access, the attacker could use it to get into systems that should only be reachable from inside the network.

The DTLS flaw can also knock the appliance offline. Remote employees could lose VPN access, and applications running through NetScaler may stop working.

Patching prevents the vulnerabilities from being used again, but it does not clean up the device. Any accounts, files, or settings added before the update will remain until they are found and removed.

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** – Upgrade every affected NetScaler appliance to the latest supported build. See Citrix's [security advisory](#) for more information:
 - 14.1-73.37 or later
 - 13.1-64.24 or later
 - 14.1-73.37 FIPS or later
 - 13.1-37.279 FIPS or NDcPP, or later
- Remove internet access or isolate any vulnerable appliance that cannot be updated immediately.
- Run the Citrix IoC scan through NetScaler Console. Contact Citrix Support if the scan is unavailable.
- Check external logs for unknown administrative sessions, unexpected outbound connections, or missing activity.
- If compromise is found, preserve the appliance snapshot and logs before remediation. Patching does not remove access established before the update.

TTPs to Watch

Initial Access

- Exploit Public-Facing Application [T1190]: Attackers exploit internet-facing NetScaler ADC and NetScaler Gateway appliances to run code without authentication. (*CVE-2026-88771 and CVE-2026-88772*)

Impact

- Network Denial of Service [T1498]: An attacker could exploit the DTLS memory overflow and make the NetScaler appliance unavailable, interrupting VPN or application access. (CVE-2026-88772)

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

These vulnerabilities impact organizations that use Citrix NetScaler ADC or NetScaler Gateway for remote access, application delivery, authentication, or load balancing.

- Public Sector
- Finance
- Healthcare
- Manufacturing
- Energy
- Education

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 any vulnerability in this notice, 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](#)

[Threat Brief: NetScaler Zero Days CVE-2026-88771 and CVE-2026-88772 Exploited in the Wild](#)