

Alert Bulletin

Bulletin N.: 110
Publication Date: 29/09/2026
Subject: Alert 2026-110 Active exploitation of 0-day vulnerabilities in Citrix
Traffic Light Protocol (TLP): White

Affected product(s):

Product	Configuration / condition	Vulnerabilities
Citrix NetScaler ADC	Default configuration	CVE-2026-8771
Citrix NetScaler Gateway	Default configuration	CVE-2026-8771
Citrix NetScaler ADC	DTLS enabled	CVE-2026-8772
Citrix NetScaler Gateway	DTLS enabled, normally enabled by default on VPN virtual servers	CVE-2026-8772
NetScaler ADC / Gateway 12.1 and 13.0	Unsupported / End of Life	No patch; requires migration to a supported release

Description

Two zero-day vulnerabilities have been published in **NetScaler ADC** and **Citrix NetScaler Gateway**: **CVE-2026-8771 (CVSSv4 9.5)** and **CVE-2026-8772 (CVSSv4 9.5)**. Both allow unauthenticated remote attackers to achieve **remote code execution (RCE)** on vulnerable appliances; the first affects deployments with the default configuration, and the second requires **DTLS** to be enabled, a feature enabled by default on VPN virtual servers. Citrix confirmed that exploitation of **CVE-2026-8771** and **CVE-2026-8772** has been observed in unmitigated NetScaler deployments.

The vulnerabilities are detailed below:

- **CVE-2026-8771 — Incorrect input validation / Pre-authentication RCE**

CVE-2026-8771 is a remote code execution vulnerability caused by insufficient input validation (**CWE-20**) in NetScaler ADC and NetScaler Gateway. It has a **CVSS v4.0 score of 9.5** and affects all vulnerable deployments, even with the default configuration; it does not require enabling any additional feature.

An unauthenticated remote attacker can send specially crafted requests to the appliance and execute arbitrary commands. The flaw requires network connectivity to the vulnerable service, but does not require credentials, user interaction, or any special configuration other than the product's standard configuration.

- **CVE-2026-8772 — Memory overflow / RCE or DoS via DTLS**

CVE-2026-8772 is a memory overflow vulnerability (**CWE-119**) that can lead to remote code execution or denial of service. It also has a **CVSS v4.0 score of 9.5**, but exposure requires **DTLS to be enabled** on NetScaler ADC or Gateway.

DTLS is enabled by default on **VPN virtual servers**, so all appliances offering VPN access should be treated as potentially affected until the configuration is verified and the patch is applied. The attack complexity reported by Citrix is high, but active exploitation increases the urgency of remediation.

Solution

The definitive solution is to install one of the fixed versions of Citrix NetScaler:

- **14.1-73.37 or later** for NetScaler ADC and Gateway 14.1.
- **13.1-64.23 or later** for NetScaler ADC and Gateway 13.1.
- **14.1-73.37 FIPS or later** for NetScaler ADC 14.1-FIPS.
- **13.1-37.279 or later** for NetScaler ADC 13.1-FIPS and 13.1-NDcPP.

Appliances on the 12.1 and 13.0 branches must migrate to a supported release, as no security update is available for those versions.

Product / branch	Minimum fixed version
NetScaler ADC and NetScaler Gateway 14.1	14.1-73.37 or later
NetScaler ADC and NetScaler Gateway 13.1	13.1-64.23 or later
NetScaler ADC 14.1-FIPS	14.1-73.37 FIPS or later
NetScaler ADC 13.1-FIPS	13.1-37.279 or later
NetScaler ADC 13.1-NDcPP	13.1-37.279 or later
NetScaler ADC / Gateway 12.1 and 13.0	Migrate to a supported version; they do not receive security updates

Before upgrading, NetScaler recommends checking free space, backing up the configuration, validating prerequisites, and downloading the applicable firmware from the official portal. For a safe upgrade, the documentation indicates that at least **7 GB of free space in /var** and **200 MB in /flash** are required for a standalone appliance; pre-upgrade validations must complete without errors before the installation begins.

For **standalone** devices, the recommended workflow is:

1. Save the current configuration with save config.
2. Back up the /nsconfig/ns.conf file and confirm available space.
3. Download and upload the firmware package corresponding to the installed branch.
4. Run the pre-upgrade validations from **System > System Upgrade** in the GUI, or ./installns –pre_check from the CLI.
5. Install the update and restart when prompted by the process.
6. Confirm the installed build, the health of the appliance, the *virtual servers*, authentication, VPN, DTLS, load balancing, and published applications.

For **High Availability (HA)** pairs, NetScaler recommends updating the **secondary node** first, forcing *failover*, and then updating the node that was previously primary. This minimizes impact and allows service continuity to be maintained during the upgrade.

Citrix has not published a *workaround* that completely eliminates CVE□2026□8771 or CVE□2026□8772; upgrading to a fixed build is the only definitive remediation. Disabling DTLS may temporarily reduce exposure to CVE□2026□8772 when it does not affect operations, but it does not protect against CVE□2026□8771.

Official links to assist with the upgrade process:

- https://support.citrix.com/external/article/CTX697096/citrix-netscaler-adc-and-citrix-netscale.html
- https://docs.netscaler.com/en-us/citrix-adc/current-release/upgrade-downgrade-citrix-adc-appliance.html
- https://docs.netscaler.com/en-us/citrix-adc/current-release/upgrade-downgrade-citrix-adc-appliance/upgrade-downgrade-before-you-begin.html
- https://docs.netscaler.com/en-us/citrix-adc/current-release/upgrade-downgrade-citrix-adc-appliance/upgrade-standalone-appliance.html
- https://docs.netscaler.com/en-us/citrix-adc/current-release/upgrade-downgrade-citrix-adc-appliance/upgrade-downgrade-ha-pair.html
- https://docs.netscaler.com/en-us/citrix-adc/current-release/upgrade-downgrade-citrix-adc-appliance/pre-upgrade-validation-checks.html

Additional information:

- https://www.bleepingcomputer.com/news/security/cisa-orders-feds-to-patch-exploited-citrix-flaws-by-wednesday/
- https://support.citrix.com/external/article/CTX697096/citrix-netscaler-adc-and-citrix-netscale.html