# Citrix NetScaler ADC and Gateway: two critical RCE flaws under active exploitation



Citrix fixed 8 vulnerabilities in customer-managed NetScaler ADC and Gateway on 27 September 2026, including two critical RCE flaws it confirms are exploited in the wild. CERT-EU urges immediate updates and compromise assessments.

- Citrix's 27 September 2026 bulletin covers 8 vulnerabilities in customer-managed NetScaler ADC and NetScaler Gateway.
- CVE-2026-88771 (CVSS 9.5) is an unauthenticated RCE with no preconditions, so it affects all deployments, and it is exploited in the wild.
- CVE-2026-88772 (CVSS 9.5) is a memory overflow leading to RCE or DoS where DTLS is enabled, which is the default on VPN vServer; it is also exploited.
- Affected builds include 13.1 before 13.1-64.23 and 14.1 before 14.1-73.37, plus FIPS and NDcPP

variants and Secure Private Access Hybrid deployments using NetScaler.

- CERT-EU advises updating immediately and running a compromise assessment on internet-facing appliances.

## What happened

On 27 September 2026 Citrix published a security bulletin covering 8 vulnerabilities in customer-managed NetScaler ADC and NetScaler Gateway. Two of them are critical, unauthenticated remote code execution flaws, and Citrix has confirmed both are being exploited in the wild. CERT-EU issued an advisory recommending prompt updates.

## Technical picture

**CVE-2026-88771** (CVSS 9.5) stems from improper input validation. It needs no precondition, so every NetScaler ADC and Gateway deployment is exposed. **CVE-2026-88772** (CVSS 9.5) is a memory overflow that can lead to RCE or denial of service where DTLS is enabled, which is the default on VPN vServer.

The remaining flaws depend on configuration. CVE-2026-88773 (CVSS 9.3) is HTTP request smuggling and CVE-2026-88774 (CVSS 7.0) a policy bypass, both tied to HTTP URL-based policy expressions. CVE-2026-88775, -88776 and -88777 (CVSS 8.8 each) are memory overflows linked to specific vServer or protocol setups, and CVE-2026-88778 (CVSS 8.8) is TCP ISN prediction where Enhanced ISN Generation is disabled.

## Affected versions

NetScaler ADC and Gateway 13.1 before 13.1-64.23 and 14.1 before 14.1-73.37 are affected. So are ADC FIPS 14.1 before 14.1-73.37 FIPS and ADC FIPS and NDcPP 13.1 before 13.1-37.279. Secure Private Access Hybrid deployments using NetScaler instances must also be upgraded. The bulletin applies only to customer-managed deployments.

CERT-EU recommends updating affected appliances immediately, enabling Enhanced ISN Generation where a TCP configuration is enabled, and running a compromise assessment on any internet-facing appliance running an affected build.

## What to do now

1. Inventory all customer-managed NetScaler ADC and Gateway appliances, including FIPS, NDcPP and Secure Private Access Hybrid instances, and compare builds with the fixed versions.
2. Upgrade affected appliances to the fixed releases immediately, prioritising internet-facing systems.
3. Run a compromise assessment on every internet-facing appliance that ran an affected build, since exploitation is confirmed.
4. Enable Enhanced ISN Generation wherever a TCP configuration is enabled.

5. Check the Citrix bulletin's precondition steps (DTLS, HTTP URL-based policy expressions, vServer types) to understand your exposure.
6. Record the event and response under your incident and vulnerability management procedures, and notify the NCA or SAMA where your obligations require.