CERT-EU

Security Advisory 2026-014

Critical Vulnerabilities in Citrix NetScaler ADC and Gateway

2026-09-27 — v1.0

TLP:CLEAR

History:

- *27/09/2026 — v1.0 – Initial publication*

Summary

On 27 September 2026, Citrix published a security bulletin addressing 8 vulnerabilities affecting customer-managed Citrix NetScaler ADC and Citrix NetScaler Gateway, among which 2 critical unauthenticated Remote Code Execution (RCE) vulnerabilities. Citrix has confirmed **active exploitation** of these 2 critical vulnerabilities in the wild [1].

CERT-EU recommends updating affected software and running a compromise assessment on those exposed on the internet.

Technical Details

The vulnerability **CVE-2026-88771**, with a CVSS score of 9.5, is an unauthenticated RCE flow due to improper input validation. As there is no precondition for the exploitation, it affects all Citrix NetScaler ADC and Citrix NetScaler Gateway deployments. It is **exploited in the wild** [1].

The vulnerability **CVE-2026-88772**, with a CVSS score of 9.5, a memory overflow vulnerability leading to RCE or Denial of Service (DoS). It affects Citrix NetScaler ADC and Citrix NetScaler Gateway deployments where DTLS is enabled (default on VPN vServer). It is **exploited in the wild** [1].

The vulnerability **CVE-2026-88773**, with a CVSS score of 9.3, is an HTTP Request Smuggling vulnerability. It affects Citrix NetScaler ADC and Citrix NetScaler Gateway deployments where an HTTP URL-based policy expression configured [1].

The vulnerability **CVE-2026-88774**, with a CVSS score of 7.0, is a feature policy bypass via HTTP URL-based expression flow. It affects Citrix NetScaler ADC and Citrix NetScaler Gateway deployments where an HTTP URL-based policy expression configured [1].

The vulnerabilities **CVE-2026-88775**, **CVE-2026-88776** and **CVE-2026-88777**, each with a CVSS score of 8.8, are memory overflow vulnerabilities leading to unpredictable or erroneous behaviour or DoS conditions. They affect Citrix NetScaler ADC and Citrix NetScaler Gateway deployments where respectively, a gateway or AAA vServer is configured, an LB vServer of type

Oracle is configured, or an LB/CS or CGNAT-LSN/NAT64 with non-HTTP L7 protocol is enabled [1].

The vulnerability **CVE-2026-88778**, with a CVSS score of 8.8, is a TCP Initial Sequence Number (ISN) prediction vulnerability. It affects Citrix NetScaler ADC and Citrix NetScaler Gateway deployments where a TCP configuration is enabled with Enhanced ISN Generation disabled [1].

Affected Products

The following products and versions are affected [1]:

- Citrix NetScaler ADC and NetScaler Gateway versions **13.1 before 13.1-64.23** and **14.1 before 14.1-73.37**.
- Citrix NetScaler ADC FIPS version **14.1 before 14.1-73.37 FIPS**
- Citrix NetScaler ADC FIPS and NDcPP version **13.1 before 13.1-37.279**

This bulletin applies to customer-managed deployments only. Secure Private Access Hybrid deployments using NetScaler instances are also affected and must be upgraded.

For precondition verification steps, refer to the Citrix bulletin [1].

Recommendations

CERT-EU recommend to update all affected customer-managed appliances to the fixed version immediately. It is also recommended to enable Enhanced ISN Generation for deployments where a TCP configuration is enabled [2].

CERT-EU strongly advise to run a compromise assessment on any internet-facing appliance running an affected build.

References

[1] https://support.citrix.com/support-home/kbsearch/article?articleNumber=CTX697096

[2] https://docs.netscaler.com/en-us/citrix-adc/current-release/system/tcp-configurations.html#enhanced-isn-generation