Security Advisory 2026-010

Critical Vulnerabilities in Citrix NetScaler ADC and NetScaler Gateway

2026-08-19 — v1.0

TLP:CLEAR

History:

- *19/08/2026 — v1.0 – Initial publication*

Summary

On 19 August 2026, Citrix published a security advisory addressing multiple critical vulnerabilities in NetScaler ADC (formerly Citrix ADC) and NetScaler Gateway (formerly Citrix Gateway) [1].

CERT-EU recommends updating affected devices as soon as possible.

Technical Details

The vulnerability **CVE-2026-19489** (CVSS: 8.8) is a memory overflow vulnerability that can lead to unpredictable behaviour or Denial of Service.

The vulnerability **CVE-2026-19490** (CVSS: 9.3) is an authentication bypass using an alternate path.

Affected Products

The following supported versions of NetScaler ADC and NetScaler Gateway are affected:

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

The vulnerability CVE-2026-19489 requires SIP ALG(Session Initiation Protocol Application Layer Gateway) to be enabled on a Large Scale NAT (LSN) group configuration.

Customers can determine if the appliance meets the precondition by inspecting their NetScaler configuration for the specified string:

```
add lsn group.*sipalg.*
```

The vulnerability CVE-2026-19490 requires the appliance to be configured as a Gateway (SSL VPN, ICA Proxy, CVPN, RDP Proxy) or an AAA virtual server. On versions 14.1-43.56 or later and 13.1-61.28 or later, the issue is applicable only when a SAML action is configured; on earlier builds and 13.1 FIPS, Gateway or AAA virtual server configuration is sufficient.

Customers can determine if the appliance meets the precondition by inspecting their NetScaler configuration for the specified string:

SAML action configuration:

```
add authentication samlAction.*
```

Auth or VPN vserver:

```
add authentication vserver .*

OR

add vpn vserver .*
```

Recommendations

CERT-EU recommends to install the relevant updated versions on affected devices as soon as possible [1].

References

[1] https://support.citrix.com/support-home/kbsearch/article?articleNumber=CTX696939