CERT-EU

**Security Advisory 2026-003**

# Multiple Vulnerabilities in Citrix NetScaler and Citrix ADC

***2026-03-23 — v1.0***

**TLP:CLEAR**

*History:*

- *23/03/2026 — v1.0 – Initial publication*

## Summary

On 23 March 2026, Citrix published a security advisory addressing multiple vulnerabilities affecting NetScaler ADC and NetScaler Gateway [1]. These vulnerabilities may lead to sensitive information disclosure and user session mix-up under specific configurations.

At the time of writing, there is no public evidence of active exploitation. It is strongly recommended updating affected gateways, prioritising internet-facing assets. It is also recommended to preserve evidence for further investigation.

## Technical Details

The advisory describes two vulnerabilities:

- The vulnerability **CVE-2026-3055**, with a CVSS score of 9.3, is an out-of-bounds read vulnerability that may result in memory overread. Successful exploitation could allow an attacker to access sensitive information from memory. This issue affects systems configured as a SAML Identity Provider (IdP) [1].
- The vulnerability **CVE-2026-4368**, with a CVSS score of 7.7, is a race condition that may lead to user session mix-up. Exploitation could allow one user to gain access to another user's session. This issue affects systems configured as a Gateway (e.g. SSL VPN, ICA Proxy, CVPN, RDP proxy) or AAA virtual server [1].

## Affected Products

The vulnerabilities affect NetScaler ADC and NetScaler Gateway versions:

- prior to 14.1-66.59
- prior to 13.1-62.23
- prior to 13.1-37.262 (FIPS and NDcPP) - only for NetScaler ADC

Citrix also identified a **known issue in builds 14.1-66.54 and 14.1-66.59** affecting STA server binding configuration. When the STA server is configured using the full path (`/scripts/ctxsta.dll`), binding may fail, impacting authentication flows [2].

Additional information is available in the vendor's advisory [1].

## Recommendations

CERT-EU strongly recommends taking the following actions:

- restrict access to NetScaler Gateway and AAA virtual servers using **network-level controls** (e.g. IP allowlisting) until updates are deployed;
- where possible, **apply Global Deny List (GDL) mitigation** which enables mitigation without reboot and can help protect appliances [2];
- identify internet-facing appliances configured as **SAML Identity Provider (IdP)** or **Gateway or AAA virtual server** and prioritise their remediation due to exposure to CVE-2026-3055 and CVE-2026-4368;
- take snapshots of the appliances **before patching them**, as these may be needed later for investigating possible exploitation attempts;
- update vulnerable appliances;
- **terminate all active and persistent sessions after patching** to prevent attackers from reusing potentially compromised session tokens:

```
kill aaa session -all
kill icaconnection -all
kill rdp connection -all
kill pcoipConnection -all
clear lb persistentSessions
```

## References

[1] https://support.citrix.com/support-home/kbsearch/article?articleNumber=CTX696300

[2] https://community.citrix.com/techzone-blogs/110_security-updates/critical-and-high-severity-updates-announced-for-netscaler-gateway-and-netscaler-adc-r1256/