Security Advisory 2025-022

Severe Vulnerabilities in Citrix Products

2025-06-18 — v1.0

TLP:CLEAR

History:

- *18/06/2025 — v1.0 – Initial publication*

Summary

On 17 June 2025, Citrix released an advisory addressing two high severity vulnerabilities in NetScaler ADC and NetScaler Gateway [1].

It is recommended updating affected assets as soon as possible.

Technical Details

The vulnerability **CVE-2025-5777**, with a CVSS score of 9.3, is due to insufficient input validation leading to memory overread. To be exploitable, NetScaler must be configured as Gateway (VPN virtual server, ICA Proxy, CVPN, RDP Proxy) OR AAA virtual server.

The vulnerability **CVE-2025-5349**, with a CVSS score of 8.7, is due to improper access control on the NetScaler Management Interface. To exploit this vulnerability, it is necessary for an attacker to have access to the NSIP address, the Cluster Management IP or the local GSLB Site IP.

Affected Products

The following products are affected [1]:

- NetScaler ADC and NetScaler Gateway 14.1 BEFORE 14.1-43.56
- NetScaler ADC and NetScaler Gateway 13.1 BEFORE 13.1-58.32
- NetScaler ADC 13.1-FIPS and NDcPP BEFORE 13.1-37.235-FIPS and NDcPP
- NetScaler ADC 12.1-FIPS BEFORE 12.1-55.328-FIPS

Note: NetScaler ADC and NetScaler Gateway versions 12.1 and 13.0 are End Of Life (EOL) and are vulnerable.

Recommendations

It is recommended updating as soon as possible to the latest version of NetScaler ADC and NetScaler Gateway.

Additionally, Citrix recommends running the following commands to terminate all active ICA and PCoIP sessions after all NetScaler appliances in the HA pair or cluster have been upgraded to the fixed builds:

```
kill icaconnection -all
kill pcoipConnection -all
```

References

[1] https://support.citrix.com/support-home/kbsearch/article?articleNumber=CTX693420&articleTitle=NetScaler_ADC_and_NetScaler_Gateway_Security_Bulletin_for_CVE_2025_5349_and_CVE_2025_5777