Security Advisory 2025-033

Critical Vulnerabilities in Citrix NetScaler Products

2025-08-26 — v1.0

TLP:CLEAR

History:

- *26/08/2025 — v1.0 – Initial publication*

Summary

On 26 August 2025, Citrix released a security advisory addressing one critical and two high severity vulnerabilities in NetScaler ADC and NetScaler Gateway [1]. Citrix warns that **exploits of the critical vulnerability, CVE-2025-7775, have been observed on unmitigated appliances**.

It is recommended to update affected assets as soon as possible.

Technical Details

The vulnerability **CVE-2025-7775**, with a CVSS score of 9.2, is due to improper restriction of operations within the bounds of a memory buffer, leading to Remote Code Execution (RCE) and/or Denial of Service [1]. To be exploitable, NetScaler must have **one of the following configurations**:

- Gateway (VPN virtual server, ICA Proxy, CVPN, RDP Proxy) or AAA virtual server
- NetScaler ADC and NetScaler Gateway 13.1, 14.1, 13.1-FIPS and NDcPP: LB virtual servers of type (HTTP, SSL or HTTP_QUIC) bound with IPv6 services or servicegroups bound with IPv6 servers
- NetScaler ADC and NetScaler Gateway 13.1, 14.1, 13.1-FIPS and NDcPP: LB virtual servers of type (HTTP, SSL or HTTP_QUIC) bound with DBS IPv6 services or servicegroups bound with IPv6 DBS servers
- CR virtual server with type HDX

The vulnerability **CVE-2025-7776**, with a CVSS score of 8.8, is due to improper restriction of operations within the bounds of a memory buffer, leading to unpredictable or erroneous behaviour and Denial of Service. To be exploitable, NetScaler must be configured as Gateway (VPN virtual server, ICA Proxy, CVPN, RDP Proxy) with PCoIP Profile bounded to it.

The vulnerability **CVE-2025-8424**, with a CVSS score of 8.7, is due to improper access control. 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, or SNIP with Management Access.

Affected Products

The following products are affected by the vulnerabilities [1]:

- NetScaler ADC and NetScaler Gateway 14.1 BEFORE 14.1-47.48
- NetScaler ADC and NetScaler Gateway 13.1 BEFORE 13.1-59.22
- NetScaler ADC 13.1-FIPS and NDcPP BEFORE 13.1-37.241-FIPS and NDcPP
- NetScaler ADC 12.1-FIPS and NDcPP BEFORE 12.1-55.330-FIPS and NDcPP

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

Recommendations

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

CVE-2025-7775

Customers can determine if they have an appliance configured as one of the following by inspecting their NetScaler Configuration for the specified strings

- An Auth Server (AAA Vserver): `add authentication vserver .*`
- A Gateway (VPN Vserver, ICA Proxy, CVPN, RDP Proxy): `add vpn vserver .*`
- LB vserver of Type HTTP_QUIC|SSL|HTTP bound with IPv6 services or servicegroups bound with IPv6 servers:

```
enable ns feature lb.*
add serviceGroup .* (HTTP_QUIC|SSL|HTTP) .*
add server .* <IPv6>
bind servicegroup <servicegroup name> <IPv6 server> .*
add lb vserver .* (HTTP_QUIC|SSL|HTTP) .*
bind lb vserver .* <ipv6 servicegroup name>
```

- LB vserver of Type HTTP_QUIC|SSL|HTTP bound with DBS IPv6 services or servicegroups bound with IPv6 DBS servers:

```
enable ns feature lb.*
add serviceGroup .* (HTTP_QUIC | SSL | HTTP) .*
add server .* <domain> -queryType AAAA
add service .* <IPv6 DBS server >
bind servicegroup <servicegroup name> <IPv6 DBS server> .*
add lb vserver .* (HTTP_QUIC | SSL | HTTP) .*
bind lb vserver .* <ipv6 servicegroup name>
```

- CR vserver with type HDX: `add cr vserver .* HDX .*`

CVE-2025-7776

Customers can determine if they have an appliance configured as Gateway (VPN vserver) with PCoIP Profile bounded to it, by inspecting their *ns.conf* file for the specified strings: `add vpn vserver .* -pcoipVserverProfileName .*`

References

[1] https://support.citrix.com/support-home/kbsearch/article?articleNumber=CTX694938&articleTitle=NetScaler_ADC_and_NetScaler_Gateway_Security_Bulletin_for_CVE_2025_7775_CVE_2025_7776_and_CVE_2025_8424