مجلس الأمن السيبراني
CYBER SECURITY COUNCIL
United Arab Emirates

Actively Exploited Vulnerability in Citrix NetScaler ADC and Gateway

Tracking #:432317641

Date:27-08-2025

TLP: WHITE

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed Citrix has disclosed a critical memory overflow vulnerability in NetScaler ADC and NetScaler Gateway which could lead to remote code execution (RCE) or denial of service (DoS).

TECHNICAL DETAILS:

Citrix has disclosed a critical memory overflow vulnerability in NetScaler ADC and NetScaler Gateway, tracked as CVE-2025-7775, which could lead to remote code execution (RCE) or denial of service (DoS).

Exploited Vulnerability Details

- CVE ID: CVE-2025-7775
- CVSS Score: Critical (9.8)
- Affected Products:
  - NetScaler ADC
  - NetScaler Gateway
- Vulnerability Type: Memory Overflow
- Impact:
  - Remote Code Execution (RCE)
  - Denial of Service (DoS)
- Exploitation Status: Confirmed active exploitation in the wild
- Attack Vector: Network-based, unauthenticated attackers may exploit the vulnerability by sending crafted requests to the vulnerable service.

Other Vulnerabilities:

- CVE-2025-7776-CVSS v4.0 Base Score: 8.8
- CVE-2025-8424- CVSS v4.0 Base Score: 8.7

Affected Versions:

- 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

Fixed Versions:

- NetScaler ADC and NetScaler Gateway 14.1-47.48 and later releases
- NetScaler ADC and NetScaler Gateway 13.1-59.22 and later releases of 13.1
- NetScaler ADC 13.1-FIPS and 13.1-NDcPP 13.1-37.241 and later releases of 13.1-FIPS and 13.1-NDcPP
- NetScaler ADC 12.1-FIPS and 12.1-NDcPP 12.1-55.330 and later releases of 12.1-FIPS and 12.1-NDcPP

Note: NetScaler ADC and NetScaler Gateway versions 12.1 and 13.0 are now End Of Life (EOL) and no longer supported. Customers are recommended to upgrade their appliances to one of the supported versions that address the vulnerabilities.

RECOMMENDATIONS:

- Apply vendor patches immediately: Upgrade to the latest secure firmware/software version released by Citrix.
- Restrict access: Limit exposure of management interfaces (e.g., HTTPS/NSIP, SNIP) to trusted internal networks only.
- Monitor logs & traffic: Actively monitor for unusual activity, including unexpected process crashes, high memory usage, or anomalous traffic patterns.
- Implement segmentation & zero trust: Ensure that NetScaler appliances are isolated from critical backend systems where possible.

Kindly circulate this information to your subsidiaries and partners as well as share with us any relevant information and findings.

The UAE Cyber Security Council extends its appreciation for the continued collaboration.

REFERENCES:

- https://support.citrix.com/support-home/kbsearch/article?articleNumber=CTX694938