مجلس الأمن السيبراني
CYBER SECURITY COUNCIL
United Arab Emirates

Actively Exploited Critical Vulnerability in NetScaler ADC

Tracking #:432317416

Date:26-06-2025

THE INFORMATION CONTAINED WITHIN IS THE PROPERTY OF THE CYBER SECURITY COUNCIL OF THE UNITED ARAB EMIRATES GOVERNMENT AND IS TO BE USED EXCLUSIVELY FOR INTELLGIENCE PURPOSES. IT MAY NOT BE USED IN ANY LEGAL OR PUBLIC MATTER WITHOUT THE EXPLICIT APPROVAL OF THE CYBER SECURITY COUNCIL

TLP: WHITE

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed that Citrix has released security updates for NetScaler ADC and NetScaler Gateway to address a critical severity vulnerability. This is a memory overflow vulnerability which leads to unintended control flow and Denial of Service, which has been actively exploited in the wild.

TECHNICAL DETAILS:

Vulnerability Details:

- **CVE-2025-6543: Improper Restriction of Operations within the Bounds of a Memory Buffer**
  - **Severity:** Critical
  - **CVSS v4.0 Base Score:** 9.2
  - **Impact:** Memory overflow vulnerability leading to unintended control flow and Denial of Service.
  - **Pre-conditions:** NetScaler must be configured as Gateway (VPN virtual server, ICA Proxy, CVPN, RDP Proxy) OR AAA virtual server.
  - **Exploitation Status:** Actively exploited.

Affected Versions:

- NetScaler ADC and NetScaler Gateway 14.1 BEFORE 14.1-47.46
- NetScaler ADC and NetScaler Gateway 13.1 BEFORE 13.1-59.19
- NetScaler ADC 13.1-FIPS and NDcPP BEFORE 13.1-37.236-FIPS and NDcPP

Fixed Versions:

- NetScaler ADC and NetScaler Gateway 14.1-47.46 and later releases
- NetScaler ADC and NetScaler Gateway 13.1-59.19 and later releases of 13.1
- NetScaler ADC 13.1-FIPS and 13.1-NDcPP 13.1-37.236 and later releases of 13.1-FIPS and 13.1-NDcPP. Customers should contact support - https://support.citrix.com/support-home/home to obtain the 13.1-FIPS and 13.1-NDcPP builds that address this issue.

RECOMMENDATIONS:

The UAE Cyber Security Council recommends applying the security updates recently released by Citrix.

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=CTX694788