مجلس الأمن السيبراني
CYBER SECURITY COUNCIL
United Arab Emirates

Security Updates- NetScaler ADC and Gateway

Tracking #:432318004

Date:14-11-2025

TLP: WHITE

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed a medium-severity vulnerability has been identified in NetScaler ADC (formerly Citrix ADC) and NetScaler Gateway (formerly Citrix Gateway).

TECHNICAL DETAILS:

A medium-severity vulnerability (CVE-2025-12101) has been identified in NetScaler ADC (formerly Citrix ADC) and NetScaler Gateway (formerly Citrix Gateway). The flaw could allow attackers to execute Cross-Site Scripting (XSS) attacks when specific configurations are enabled, such as Gateway (VPN virtual server, ICA Proxy, CVPN, RDP Proxy) or AAA virtual server modes.

Successful exploitation could allow an attacker to execute arbitrary JavaScript code in the context of a user's browser session, potentially leading to session hijacking, credential theft, or redirection to malicious sites.

Vulnerability Details

- **CVE-2025-12101**
- **Vulnerability Type:** Cross-Site Scripting (XSS)
- **CWE ID:** CWE-79 – Improper Neutralization of Input During Web Page Generation
- **CVSS v4.0 Score:** 5.9 (Medium)

Description:

- A Cross-Site Scripting (XSS) vulnerability exists in NetScaler ADC and NetScaler Gateway.
- The flaw allows attackers to inject and execute malicious JavaScript code in the browser of a logged-in user.
- Successful exploitation could lead to session hijacking, credential theft, or redirection to malicious websites.

Preconditions for Exploitation:

- The appliance must be configured as one of the following:
  - Gateway mode: VPN virtual server, ICA Proxy, CVPN, or RDP Proxy
  - AAA virtual server (authentication server)

Affected Versions:

- 14.1 before 14.1-56.73
- 13.1 before 13.1-60.32
- 13.1-FIPS and 13.1-NDcPP before 13.1-37.250
- 12.1-FIPS and 12.1-NDcPP before 12.1-55.333
- Versions 12.1 and 13.0 are End-of-Life (EOL) and remain vulnerable

Fixed Versions:

- 14.1-56.73 and later
- 13.1-60.32 and later
- 13.1-37.250 (FIPS/NDcPP) and later
- 12.1-55.333 (FIPS/NDcPP) and later
- Older versions-Upgrade appliances to one of the supported versions that address the vulnerabilities.

RECOMMENDATIONS:

The UAE Cyber Security Council recommends to upgrade NetScaler ADC and NetScaler Gateway to Fixed Versions.

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=CTX695486