Computer Emergency Response Team of Mauritius

A Department of the Ministry of Information Technology, Communication and Innovation

CERT-MU Security Alert

Date of Issue: 27 August 2025

Citrix NetScaler ADC and NetScaler Gateway Vulnerabilities

Severity: Critical

System Affected:

- 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

Description

Critical vulnerabilities have been discovered in NetScaler ADC (formerly Citrix ADC) and NetScaler Gateway (formerly Citrix Gateway). One of the vulnerabilities, CVE-2025-7775, a memory overflow bug was actively exploited in attacks as a zero-day vulnerability.

In addition to the Remote Code Execution flaw, two other vulnerabilities – a memory overflow vulnerability (CVE-2025-7776), and an improper access control vulnerability on the NetScaler Management Interface (CVE-2025-8424) were detected. Successful exploitation of these vulnerabilities can lead to unauthenticated, remote code execution on vulnerable devices.

CERT-MU advises organisations to watch out for these vulnerabilities and apply fixes accordingly.

Workaround

As there are no mitigations, admins are strongly recommended to install the latest updates as soon as possible:

- 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

More details are available on:
https://support.citrix.com/support-home/kbsearch/article?articleNumber=CTX694938

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.

Report Cyber Incidents

Report cyber security incident on the **Mauritian Cybercrime Online Reporting System (MAUCORS - http://maucors.govmu.org/)**

Contact Information

Computer Emergency Response Team of Mauritius (CERT-MU)
Hotline No: (+230) 800 2378
Gen. Info. : contact@cert.govmu.org
Incident: incident@cert.govmu.org
Website: http://cert-mu.org.mu
MAUCORS+: http://maucors.govmu.org