مجلس الأمن السيبراني
CYBER SECURITY COUNCIL
United Arab Emirates

Security Updates- NetScaler ADC and NetScaler Gateway

Tracking #:432319230

Date:02-07-2026

TLP: WHITE

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed Citrix has released a security bulletin addressing six high-severity vulnerabilities affecting NetScaler ADC and NetScaler Gateway.

TECHNICAL DETAILS:

Citrix has released a security bulletin addressing six high-severity vulnerabilities affecting NetScaler ADC and NetScaler Gateway. These vulnerabilities may allow unauthenticated attackers to perform arbitrary file reads, trigger memory corruption, cause denial-of-service (DoS) conditions, or disclose sensitive information through out-of-bounds memory reads, depending on the affected feature and deployment configuration.

Vulnerability Details:

CVE ID	Vulnerability Description	Preconditions	CWE	CVSS v4.0
CVE-2026-8451	Insufficient input validation leading to an out-of-bounds memory read.	NetScaler ADC or NetScaler Gateway configured as a SAML Identity Provider (IdP).	CWE-125: Out-of-bounds Read	8.8 (High)
CVE-2026-8452	Memory overflow vulnerability leading to unpredictable behavior and Denial of Service (DoS).	Appliance configured as Gateway (SSL VPN, ICA Proxy, CVPN, RDP Proxy) or AAA Virtual Server.	CWE-119: Improper Restriction of Operations within the Bounds of a Memory Buffer	8.8 (High)
CVE-2026-8655	Multiple memory overflow vulnerabilities leading to unpredictable behavior and Denial of Service (DoS).	NetScaler ADC configured as an Oracle Load Balancer, DNS Proxy, or DNS Recursive Resolver deployment.	CWE-119: Improper Restriction of Operations within the Bounds of a Memory Buffer	8.8 (High)
CVE-2026-10816	Unauthenticated arbitrary file read vulnerability.	Access to NSIP, Cluster Management IP, or SNIP with management access enabled.	CWE-73: External Control of File Name or Path	7.1 (High)
CVE-2026-10817	Insufficient input validation leading to an out-of-bounds memory read.	TCP Timestamp enabled in a TCP Profile associated with an LB, CS, or VPN virtual server, or an associated service.	CWE-125: Out-of-bounds Read	6.9 (Medium)

CVE-2026-13474	Denial of Service via malformed HTTP/2 requests.	HTTP/2 enabled in an HTTP Profile associated with an LB, CS, or VPN virtual server, or an associated service.	CWE-401: Missing Release of Memory after Effective Lifetime	8.7 (High)

Affected Products:
The following supported versions are affected:

- NetScaler ADC and NetScaler Gateway 14.1 prior to 14.1-72.61
- NetScaler ADC and NetScaler Gateway 13.1 prior to 13.1-63.18
- NetScaler ADC 14.1 FIPS prior to 14.1-72.61 FIPS
- NetScaler ADC 13.1 FIPS and NDcPP prior to 13.1-37.272
- Secure Private Access Hybrid deployments using affected NetScaler instances

Fixed Versions:

- NetScaler ADC and NetScaler Gateway 14.1-72.61 and later releases
- NetScaler ADC and NetScaler Gateway 13.1-63.18 and later releases of 13.1
- NetScaler ADC 14.1-FIPS 14.1-72.61 FIPS and later releases of 14.1-FIPS
- NetScaler ADC 13.1-FIPS and 13.1-NDcPP 13.1.37.272 and later releases of 13.1-FIPS and 13.1-NDcPP

RECOMMENDATIONS:

Immediate Actions:

- Upgrade all affected NetScaler ADC and NetScaler Gateway appliances to the latest supported firmware.
- Apply the additional HTTP/2 configuration required to fully mitigate CVE-2026-13474.

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=CTX696604