

Alert Bulletin

Bulletin N.:

Publication Date: 14/08/2026

Subject: Alert 2026-90 Vulnerability in NetScaler ADC and NetScaler Gateway

Traffic Light Protocol (TLP): Amber

Affected product(s):

- NetScaler ADC
 - NetScaler ADC 14.1 earlier than **14.1-72.61**.
 - NetScaler ADC 13.1 earlier than **13.1-63.18**.
 - NetScaler ADC 14.1 FIPS earlier than **14.1-72.61**.
- NetScaler Gateway
 - NetScaler Gateway 14.1 earlier than **14.1-72.61**.
 - NetScaler Gateway 13.1 earlier than **13.1-63.18**.

Description

NetScaler released a security update to address **CVE-2026-8452 (CVSS 9.8)**, a **Memory Overflow** vulnerability affecting **NetScaler ADC and NetScaler Gateway**.

The vulnerability may cause unpredictable or faulty behavior of the appliance and **Denial of Service (DoS)** conditions when the vulnerable device is configured as a Gateway or AAA virtual server.

The flaw has been associated with: **CWE-119 – Improper Restriction of Operations within the Bounds of a Memory Buffer**

This category includes vulnerabilities where certain operations performed on memory are not properly restricted within the bounds of the corresponding buffer.

A remote attacker can interact with a vulnerable appliance over the network and trigger the overflow condition without the need for valid credentials or requiring user interaction. Since NetScaler Gateway is frequently used as a remote access point to enterprise infrastructure, an interruption caused by this vulnerability can directly affect VPN services, remote access, and published applications

Solution

NetScaler recommends immediately updating affected appliances to a version that includes the fix:

- NetScaler ADC and NetScaler Gateway 14.1
 - **14.1-72.61 or later**
- NetScaler ADC and NetScaler Gateway 13.1
 - **13.1-63.18 or later**
- NetScaler ADC 14.1 FIPS
 - **14.1-72.61 FIPS or later**
- NetScaler ADC 13.1 FIPS / NDcPP
 - **13.1-37.272 or later**

Additional information:

- [NVD – CVE-2026-8452](#)
- [NetScaler – Identification and remediation of CVE-2026-8452](#)
- [Canadian Centre for Cyber Security – AV26-645](#)