

# CISA Alerts to Memory Buffer Vulnerability in Citrix NetScaler ADC and Gateway

CISA has published an advisory for CVE-2026-88779, a memory buffer vulnerability in Citrix NetScaler ADC and Gateway products that may lead to denial of service.

- CVE-2026-88779 affects Citrix NetScaler ADC and Citrix NetScaler Gateway with improper memory buffer restriction
- The vulnerability could enable denial of service attacks against affected systems
- CISA directs organisations to apply vendor mitigations and evaluate internet exposure of affected assets
- Institutions must follow risk-based patching guidance or discontinue use if mitigations are unavailable

## Vulnerability Overview

The United States Cybersecurity and Infrastructure Security Agency has issued an advisory concerning **CVE-2026-88779**, a vulnerability affecting Citrix NetScaler ADC (formerly Citrix ADC) and Citrix NetScaler Gateway (formerly Citrix Gateway). The flaw involves improper restriction of operations within the bounds of a memory buffer, a condition that could be exploited to cause denial of service on vulnerable systems.

## Required Actions and Compliance Guidance

CISA directs organisations to apply mitigations in accordance with vendor instructions. The advisory references CISA's BOD 26-04 guidance on prioritising security updates based on risk, as well as forensics triage requirements. Stakeholders are instructed to evaluate the internet exposure of each affected asset and ensure adherence to the binding operational directive's patching guidelines. Where mitigations are not available, organisations should follow applicable guidance for cloud services or discontinue use of the product.

## Implications for Saudi Institutions

Regulated institutions in the Kingdom that deploy Citrix NetScaler products in application delivery or secure remote access roles should review their inventories immediately. Given the potential for service disruption,

organisations must assess whether affected systems are internet-facing and prioritise remediation accordingly. Coordination with vendors and internal security teams is essential to maintain operational resilience while addressing this vulnerability in line with risk-based frameworks.

## **What to do now**

1. Identify all Citrix NetScaler ADC and Gateway deployments across your environment and document their versions
2. Assess whether affected systems are internet-facing or exposed to untrusted networks
3. Contact Citrix or your authorised reseller to obtain vendor-specific mitigation guidance and patches
4. Apply vendor-recommended mitigations or patches in accordance with your change management and risk assessment processes
5. If mitigations are unavailable, evaluate alternative controls or discontinue use of affected products until remediation is possible
6. Document remediation actions and timelines for audit and compliance purposes in line with NCA and SAMA requirements