



BGD e-GOV CIRT

TLP: CLEAR



CYBER THREAT ALERT

**Active Exploitation of Critical
Vulnerabilities Affecting Citrix
NetScaler ADC and NetScaler
Gateway**



[THIS PAGE IS INTENTIONALLY LEFT BLANK]

BGD e-GOV CIRT

TLP: CLEAR

Distribution: Public

Alert on: Active Exploitation of Critical Vulnerabilities Affecting Citrix NetScaler ADC and NetScaler Gateway

Threat Status: Active Exploitation Observed

Severity: **Critical**

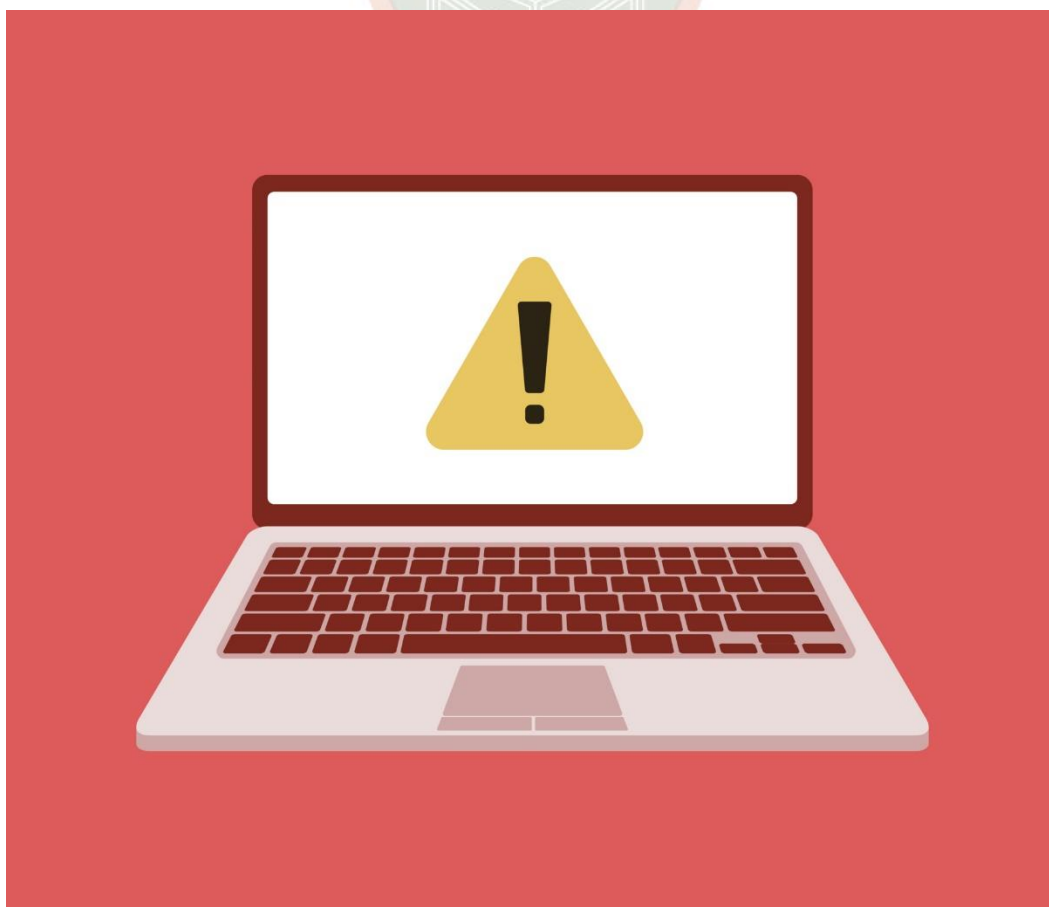
Date: 29 September 2026

Executive Summary

The Cyber Threat Intelligence (CTI) Unit of BGD e-GOV CIRT is warning organizations across Bangladesh of the **active exploitation of multiple vulnerabilities affecting Citrix NetScaler ADC and NetScaler Gateway**.

Citrix has disclosed **eight vulnerabilities (CVE-2026-88771 through CVE-2026-88778)**. Of these, **CVE-2026-88771 and CVE-2026-88772 are confirmed to be actively exploited in the wild**, with both rated CVSS 4.0: **9.5 (Critical)**. CVE-2026-88771 is particularly significant as it can allow **unauthenticated remote code execution without requiring any additional feature to be enabled**.

Organizations operating internet-facing NetScaler appliances, particularly those supporting **VPN, remote access, authentication or application delivery**, are advised to treat this as an **urgent remediation priority**.



Vulnerabilities

CVE	Severity	Description	Key Precondition	Exploitation Status
CVE-2026-88771	Critical – 9.5	A remote code execution vulnerability exists due to improper input validation, which can allow an unauthenticated attacker to execute arbitrary commands	No additional feature required	Yes
CVE-2026-88772	Critical – 9.5	Memory overflow vulnerability leading to Remote Code Execution or Denial of Service	DTLS enabled	Yes
CVE-2026-88773	Critical – 9.3	HTTP request smuggling	Specific HTTP/SSL configurations	Not reported
CVE-2026-88774	High – 7.0	Feature policy bypass due to improper HTTP URL based expression usage	HTTP URL-based expression	Not reported
CVE-2026-88775	High – 8.8	Memory overflow vulnerability leading to unpredictable or erroneous behavior or Denial of Service	Gateway/AAA configurations	Not reported
CVE-2026-88776	High – 8.8	Memory overflow vulnerability leading to unpredictable or erroneous behavior or Denial of Service	Oracle Load Balancing configuration	Not reported
CVE-2026-88777	High – 8.8	Memory overflow vulnerability leading to unpredictable or erroneous behavior or Denial of Service	Specific non-HTTP Layer 7 configurations	Not reported
CVE-2026-88778	High – 8.8	TCP Initial Sequence Number (ISN) prediction	Enhanced ISN Generation disabled	Not reported

Affected Versions

These vulnerabilities affect the following supported versions of Citrix NetScaler ADC and Citrix NetScaler Gateway:

- *Citrix NetScaler ADC and Citrix NetScaler Gateway 14.1 BEFORE 14.1-73.37*
- *Citrix NetScaler ADC and Citrix NetScaler Gateway 13.1 BEFORE 13.1-64.23*
- *Citrix NetScaler ADC FIPS BEFORE 14.1-73.37 FIPS*
- *Citrix NetScaler ADC FIPS and NDcPP BEFORE 13.1-37.279*

Potential Risks and Impact

Exploitation of these vulnerabilities could allow attackers to execute unauthorized commands, compromise NetScaler appliances, bypass security controls, and gain access to protected services. Potential impacts include:

- **Remote Code Execution:** Unauthorized control of vulnerable appliances.
- **Data & Credential Exposure:** Theft of credentials, sessions, or sensitive information.
- **Network Compromise:** Use of NetScaler as an entry point for lateral movement.
- **Service Disruption:** Denial of service affecting VPN, remote access, and applications.
- **Persistent Access:** Establishment of unauthorized access for further compromise.

Immediate Actions

1. Confirm Exposure

Follow Citrix's "**Steps to determine if an appliance meets the CVE preconditions**" to identify vulnerable systems and determine whether the affected configurations are present.

2. Isolate

Where feasible, **isolate vulnerable NetScaler appliances from untrusted networks**, particularly Internet-facing systems, until investigation and remediation are complete.

3. Preserve Evidence Before Remediation

If an appliance is exposed or compromise is suspected, **preserve evidence before upgrading or rebooting it**.

Capture:

- NetScaler VPX instance snapshot
- Remote Syslog and NetScaler Console logs
- Technical Support Bundle
- Packet Engine core dump

This is important because remediation may alter or remove forensic evidence.

4. Hunt for Compromise

Review the appliance and associated infrastructure for:

- Suspicious administrative sessions
- Unexpected outbound connections
- Unexplained gaps in logging
- Unexpected configuration or file changes
- Unusual authentication activity
- Unknown or suspicious source IP addresses

- Organizations should use the **Citrix NetScaler Console IoC detection capability** for an initial assessment of potentially compromised deployments. The feature is available through the **NetScaler Console Security Advisory** workflow from **version 14.1-73.36**, subject to the required prerequisites, including an enabled telemetry channel. Organizations that do not use NetScaler Console should **contact Citrix Support to obtain assistance with the applicable IoCs and scanning**.

Important: A clean IoC scan **does not confirm that an appliance is uncompromised**. Citrix notes that the available IoCs do not cover all possible attacker **Tactics, Techniques and Procedures (TTPs)** and may have limited forensic value. Organizations should therefore consider further investigation where compromise is suspected.

5. Patch

Upgrade affected appliances to latest available versions (Check Citrix blog for more details).

6. Rotate and Monitor

After remediation:

- **Rotate** passwords, credentials, secrets, and certificates associated with the affected appliance.
- **Maintain enhanced monitoring** for suspicious administrative activity, unexpected outbound connections, and other anomalous behavior.
- **Keep NetScaler management interfaces off the public Internet** and restrict access to trusted administrative networks.

7. Report Incidents

Report or inform BGD e-GOV CIRT regarding any cyber incident, IOC's, suspicious activities within your infrastructure, through mail id: cirt@cirt.gov.bd

References:

1. <https://support.citrix.com/support-home/kbsearch/article?articleNumber=CTX697096>
2. <https://labs.watchtower.com/oh-look-the-foot-gun-went-off-again-citrix-netscaler-preauth-command-injection-cve-2026-88771/>
3. <https://unit42.paloaltonetworks.com/netscaler-zero-days-exploited/>