contact@namiq.io · namiq.io

NamiQ

SECURITY ADVISORY

Citrix NetScaler exploited

CVE-2026-88779 · on CISA's exploited list since 4 October 2026

Analysis Report

If you run NetScaler ADC or Gateway, act now: CISA's 7 October 2026 deadline has passed. First list every appliance and its build, then ask your IT provider to confirm each one against the affected …

PREPARED BY	NamiQ	DATE	1 November 2026
FACTS AS OF	1 November 2026	VERSION	1.0
SEVERITY	**High: CVSS 4.0 8.7**	STATUS	On CISA's exploited list; due 7 October 2026

NamiQ © 2026 NamiQ. All rights reserved. This document is the property of NamiQ. It may be shared unaltered, with attribution.
Companion article: namiq.io/insights/citrix-netscaler-cve-2026-88779

The bottom line

> *If you run NetScaler ADC or Gateway, act now: CISA's 7 October 2026 deadline has passed. First list every appliance and its build, then ask your IT provider to confirm each one against the affected builds in the record.*

At a glance

Fact	Detail
Product	Citrix NetScaler (CVE-2026-88779)
Severity	High: 8.7 (CVSS 4.0)
CISA	On its exploited list since 4 October 2026. Deadline for US federal agencies: 7 October 2026.
Chance of exploitation (EPSS)	0.11, the estimated chance in the next 30 days, as at 1 November 2026
Ransomware use	Not recorded by CISA. That is not the same as none.
Fixed in	The record's affected ranges end before 14.1-73.41, 13.1-64.28, 14.1-73.41 FIPS, 13.1-37.282
Who looks first	Anyone running NetScaler ADC (including FIPS builds) or NetScaler Gateway, formerly Citrix ADC and Citrix Gateway. Usually your IT provider or network team runs these, so ask them first.

Does this apply to you?

Answer in order. Stop at the first no.

Question	If no	If yes
Do you run Citrix NetScaler ADC or NetScaler Gateway, or did you in the past as Citrix ADC or Gateway?	Nothing to do for this CVE.	Find the build on each appliance (next question).
Is any build older than the affected limits in the record for your 14.1 or 13.1 line?	This CVE does not apply to that appliance; keep a note of the build.	Treat it as affected and arrange the update now.
Can anyone outside your own network reach the appliance?	Exposure is lower, but still update; the record states no condition for an attack.	Make this your first update, ahead of routine patching.

What it is

CISA says a memory-buffer flaw in NetScaler ADC and Gateway could allow a denial of service, meaning the appliance could stop serving users. The record does not say whether an attacker needs to log in first.

Why it matters

Our reading: a denial of service on this kind of appliance is an outage, and the record names no condition that limits it. The record's score is 8.7 (CVSS 4.0), and CISA lists the flaw as exploited. CISA's page does not say how it is being used, so plan for an outage and check the system for signs of misuse.

Things people will get wrong

- "It is only a denial of service, so it can wait." CISA lists it as exploited and its deadline has passed. An outage on a gateway or load balancer stops your users working.
- "Our version is not listed, so we are safe." The record lists builds by limit, such as before 14.1-73.41. Compare your exact build against those limits, not just the product name.
- "Citrix ADC is a different product." CISA says NetScaler ADC was formerly Citrix ADC, and NetScaler Gateway was formerly Citrix Gateway. The old names are covered.

How we would triage it

This is our judgement.

The commands only read: they print a version or list what is installed. They come from general knowledge of this kind of product, not from the sources, so check them against the vendor's page before you run them. Words in capitals are for you to fill in.

Step 1: Find every appliance and its build

- List each NetScaler ADC and Gateway you run, including FIPS builds and any run by a provider, because the record lists FIPS builds separately.
- Record the exact build string from each one and compare it with the limits in the record.

```
show ns version
```

Step 2: Reduce exposure while you wait

- Ask which management and Gateway addresses are reachable from the internet and whether they need to be.
- The sources do not name a workaround, so do not rely on one; the update is the fix.

```
show ns ip
show vpn vserver
```

Step 3: Update to an unaffected build

- No source we could read names the fixed version. Ask the vendor or your provider for the build that is not affected and the vendor's instructions.
- Follow the vendor's instructions, as CISA's required action says.

Step 4: Confirm and check for misuse

- Get written confirmation of the build on each appliance after the update.
- Review appliance logs and CISA's forensic triage requirements, because the flaw is listed as exploited.

To close it, read the version from the product itself, not from an old inventory, and save the output with the date. If you cannot update today, write down who owns it, the new date, and what limits exposure until then.

Send this to your IT provider

Copy it, change the names and dates, and send it. It is a draft for you to check, not a template tested with any provider.

> *Hello, we need to confirm our exposure to CVE-2026-88779 in Citrix NetScaler ADC and NetScaler Gateway (formerly Citrix ADC and Citrix Gateway). Please tell us whether we run any, where they are, and the exact build of each. CISA's deadline of 7 October 2026 has passed, so please also tell us the build each needs and the vendor's update instructions. Please confirm in writing by the end of this week the build on each appliance and that the fix is in place.*

Signs it was used

An update closes the hole. It does not tell you whether someone used it first. CISA's required action points to its forensic triage requirements (BOD 26-04). Look for:

- Unplanned restarts or crashes of the appliance, which would fit a denial of service.
- Unusual or repeated requests to the appliance from addresses you do not recognise, around any outage.
- Changes to its configuration or accounts that nobody on your team made.

The weakness behind it

CISA's entry classes this as CWE-119 (Improper Restriction of Operations within the Bounds of a Memory Buffer).

The sources, in their words

CISA's catalogue entry:

> *Citrix NetScaler ADC (formerly Citrix ADC) and Citrix NetScaler Gateway (formerly Citrix Gateway) contain an improper restriction of operations within the bounds of a memory buffer vulnerability that could allow for a denial of service.*

The CVE record, published by NetScaler on 4 October 2026:

> *Vulnerability in NetScaler ADC and NetScaler Gateway. This issue affects ADC: before 14.1-73.41, before 13.1-64.28, before 14.1-73.41 FIPS, and before 13.1-37.282; Gateway: before 14.1-73.41 and before 13.1-64.28.*

Versions of NetScaler ADC the record lists as affected:

- all versions before 14.1-73.41
- all versions before 13.1-64.28
- all versions before 14.1-73.41 FIPS
- all versions before 13.1-37.282

The affected ranges end before 14.1-73.41, 13.1-64.28, 14.1-73.41 FIPS, 13.1-37.282. Those are the first versions the record does not list as affected; confirm them in the vendor's advisory.

Versions of NetScaler Gateway the record lists as affected:

- all versions before 14.1-73.41
- all versions before 13.1-64.28

The affected ranges end before 14.1-73.41, 13.1-64.28. Those are the first versions the record does not list as affected; confirm them in the vendor's advisory.

CISA's required action:

> *Apply mitigations in accordance with vendor instructions, ensuring compliance with CISA's BOD 26-04 Prioritizing Security Updates Based on Risk (see URL in Notes) guidance and CISA's "Forensics Triage Requirements" (see URL in Notes).*

What we do not know yet

- Which build is the first unaffected one; no source we could read names a fixed version.
- Whether an attacker needs to log in or only needs network access to the appliance.
- Whether any workaround exists short of updating.
- How the flaw is being used against victims; CISA's listing does not say.
- We have not tested this against any environment. Versions and scores are as the sources state them and as at 1 November 2026; the vendor's advisory wins where it differs.
- The sections headed "The bottom line", "Does this apply to you?", "What it is", "Why it matters", "Exposure by situation", "Things people will get wrong", "How we would triage it" and "Send this to your IT provider" are our interpretation of the sources, not a statement by CISA or the vendor.

Appendix 1. Severity decoded

CVE-2026-88779: score 8.7, `CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:N/VI:N/VA:H/SC:N/SI:N/SA:N` As the CVE record gives it. The record's own score can differ from the base score on the NVD record.

Metric	Value	What it means here
Attack vector	Network	Reachable over a network, with no need to be on the same segment.
Attack complexity	Low	No special conditions beyond the flaw itself.
Attack requirements	None	Works against a default deployment.
Privileges required	None	No account is needed.
User interaction	None	No one has to do anything.
Vulnerable system: confidentiality	None	No data exposed.
Vulnerable system: integrity	None	Nothing can be altered.
Vulnerable system: availability	High	Total loss of availability.
Subsequent systems: confidentiality	None	No data exposed.
Subsequent systems: integrity	None	Nothing can be altered.
Subsequent systems: availability	None	No effect on availability.

Appendix 2. Timeline

Date	Event
4 October 2026	CVE record published by NetScaler.
4 October 2026	CISA added it to its list of exploited vulnerabilities.
7 October 2026	CISA's deadline for US federal agencies.

Appendix 3. Exposure by situation

These priorities are our judgement from the attacker prerequisites in the sources. They are not vendor ratings.

Your situation	Priority	Timeframe

An appliance on an affected build that is reachable from the internet	High	Now; CISA's window has already passed
An affected build reachable only from inside your network	Medium	This week
You cannot tell which build is running or who manages it	High	Find out today, then decide
An appliance already past the affected limits in the record	Low	Keep a record of the build; no action for this CVE
You do not run NetScaler or Citrix ADC or Gateway	None	None for this CVE

Appendix 4. Definition of done

- Every Citrix NetScaler you run is listed, with its version.
- Each is outside the affected list, or the vendor's mitigation is in place.
- The version output or a screenshot is saved with the date.
- Logs for the weeks before the update were searched, and anything odd was written down.
- Anything not done has an owner and a date.

Sources

- CISA Known Exploited Vulnerabilities catalogue: https://www.cisa.gov/known-exploited-vulnerabilities-catalog
- CVE record for CVE-2026-88779: https://www.cve.org/CVERecord?id=CVE-2026-88779
- FIRST: Exploit Prediction Scoring System: https://www.first.org/epss/
- Reference in the CVE record: support.citrix.com: https://support.citrix.com/support-home/kbsearch/article?articleNumber=CTX697174