

CVE-2026-8452

Citrix NetScaler ADC and NetScaler Gateway Improper Restriction of Operations within the Bounds of a Memory Buffer Vulnerability

CISA KEV since Aug 26, 2026

Actively exploited

Memory overflow vulnerability NetScaler ADC and NetScaler Gateway leading to unpredictable or erroneous behavior and Denial of Service if the appliance is configured as a Gateway (SSL VPN, ICA Proxy, CVPN, RDP Proxy) or AAA virtual server

EVRS 75 / ₁₀₀ Urgent priority	CVSS V4.0 8.8 High · NVD	EPSS 0.010 62.8th percentile · FIRST	CISA DEADLINE Aug 29, 2026 CISA federal deadline · Overdue by 54 days
---	--	--	---

Signals behind the score

☒ counted in the score ☐ not counted

evidence for 6 of 8 signals

☒ CISA KEV	Listed in the catalog	☐ Vendor exploitation	Confirmed exploitation in the wild
☐ Ransomware	No known ransomware campaign association	☒ KEV recency	Added to CISA KEV within the last 90 days
☒ EPSS	0.010 probability	☐ Pre-patch disclosure	Disclosure status unavailable
☒ CVSS	Base score 8.8	☐ Microsoft Exploitability Index	Not a Microsoft CVE

Remediation

Patch This Cycle Patch or fixed version identified

CISA 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). Follow applicable BOD 26-04 guidance for cloud services or discontinue use of the product if mitigations are unavailable. Stakeholders are responsible for evaluating each asset's internet exposure and ensuring adherence to BOD 26-04 patching guidelines.

Basis: CISA KEV required action

Affected and fixed versions

PACKAGE	AFFECTED	FIXED IN	SOURCE
netScaler application delivery controller	< 13.1-37.272 ≥ 13.1 < 13.1-63.18 ≥ 14.1 < 14.1-72.61 14.1-66.68	13.1-37.272 · 13.1-63.18 · 14.1-72.61	NVD
netScaler gateway	≥ 13.1 < 13.1-63.18 ≥ 14.1 < 14.1-72.61	13.1-63.18 · 14.1-72.61	NVD

Sources

Vendor guidance	github.com/advisories/GHSA-r7wg-r5wj-c765	Additional guidance	support.citrix.com/support-home/kbsearch/article?articleNumber=CTX696604
BOD 26-04	cisa.gov/news-events/directives/bod-26-04-prioritizing-security-updates-based-risk	Forensics Triage Requirements	cisa.gov/news-events/directives/bod-26-04-implementation-guidance-prioritizing-security-updates-based-risk
NVD	nvd.nist.gov/vuln/detail/CVE-2026-8452	CISA KEV	cisa.gov/known-exploited-vulnerabilities-catalog
ENISA EUVD	euvd.enisa.europa.eu/vulnerability/EUVD-2026-40307	Current data	evulnable.com/vulnerability-management/cve/CVE-2026-8452

Snapshot at generation time. EPSS can move quickly. A public exploit module is not evidence of active exploitation.