

CVE-2025-6543

Citrix NetScaler ADC and Gateway Buffer Overflow Vulnerability

CISA KEV since Jun 30, 2025

Actively exploited

Memory overflow vulnerability leading to unintended control flow and Denial of Service in NetScaler ADC and NetScaler Gateway when configured as Gateway (VPN virtual server, ICA Proxy, CVPN, RDP Proxy) OR AAA virtual server

EVRS 75 / ₁₀₀ Urgent priority	CVSS V4.0 9.2 Critical · NVD	EPSS 0.106 95.8th percentile · FIRST	CISA DEADLINE Jul 21, 2025 KEV since 2025 · listed over a year
---	--	--	--

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 two years
☒ EPSS	0.106 probability	☐ Pre-patch disclosure	Disclosure status unavailable
☒ CVSS	Base score 9.2	☐ Microsoft Exploitability Index	Not a Microsoft CVE

Remediation

Patch This Cycle Patch or fixed version identified

CISA required action: Apply mitigations per vendor instructions, follow applicable BOD 22-01 guidance for cloud services, or discontinue use of the product if mitigations are unavailable.

Basis: CISA KEV required action

Affected and fixed versions

PACKAGE	AFFECTED	FIXED IN	SOURCE
netScaler application delivery controller	$\geq 13.1 < 13.1-37.236$ $\geq 13.1 < 13.1-59.19$ $\geq 14.1 < 14.1-47.46$	$13.1-37.236 \cdot 13.1-59.19 \cdot 14.1-47.46$	NVD
netScaler gateway	$\geq 13.1 < 13.1-59.19$ $\geq 14.1 < 14.1-47.46$	$13.1-59.19 \cdot 14.1-47.46$	NVD

Sources

Vendor guidance	github.com/advisories/GHSA-9gqr-6728-fpv3	Additional guidance	support.citrix.com/support-home/kbsearch/article?articleNumber=CTX694788
netScaler.com	netScaler.com/blog/news/netScaler-critical-security-updates-for-cve-2025-6543-and-cve-2025-5777/	NVD	nvd.nist.gov/vuln/detail/CVE-2025-6543
CISA KEV	cisa.gov/known-exploited-vulnerabilities-catalog	ENISA EUVD	euvd.enisa.europa.eu/vulnerability/EUVD-2025-19085
Current data	evulnable.com/vulnerability-management/cve/CVE-2025-6543		

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