

CVE-2025-5777

Citrix NetScaler ADC and Gateway Out-of-Bounds Read Vulnerability

Exigent

CISA KEV since Jul 10, 2025

Actively exploited

Ransomware use known

Insufficient input validation leading to memory overread when the NetScaler is configured as a Gateway (VPN virtual server, ICA Proxy, CVPN, RDP Proxy) OR AAA virtual server

EVRS 94 /100 Immediate priority	CVSS V4.0 9.3 Critical · NVD	EPSS 0.999 99.98th percentile · FIRST	CISA DEADLINE Jul 11, 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	Known ransomware campaigns	☐ KEV recency	Added to CISA KEV within the last two years
☒ EPSS	0.999 probability	☐ Pre-patch disclosure	Disclosure status unavailable
☒ CVSS	Base score 9.3	☐ Microsoft Exploitability Index	Not a Microsoft CVE

Remediation

Out-of-band / urgent 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	$\geq 12.1 < 12.1-55.328$ $\geq 13.1 < 13.1-37.235$ $\geq 13.1 < 13.1-58.32$ $\geq 14.1 < 14.1-43.56$	$12.1-55.328 \cdot 13.1-37.235 \cdot 13.1-58.32 \cdot 14.1-43.56$	NVD
netScaler gateway	$\geq 13.1 < 13.1-58.32$ $\geq 14.1 < 14.1-43.56$	$13.1-58.32 \cdot 14.1-43.56$	NVD

Sources

Vendor guidance github.com/advisories/GHSA-29vj-j5w5-pcph

Additional guidance support.citrix.com/support-home/kbsearch/article?articleNumber=CTX693420

NVD nvd.nist.gov/vuln/detail/CVE-2025-5777

CISA KEV cisa.gov/known-exploited-vulnerabilities-catalog

ENISA EUVD euvd.enisa.europa.eu/vulnerability/EUVD-2025-18497

Current data evulnable.com/vulnerability-management/cve/CVE-2025-5777

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