

CVE-2023-6549

Citrix NetScaler ADC and NetScaler Gateway Buffer Overflow Vulnerability

CISA KEV since Jan 17, 2024

Actively exploited

Improper Restriction of Operations within the Bounds of a Memory Buffer in NetScaler ADC and NetScaler Gateway allows Unauthenticated Denial of Service and Out-Of-Bounds Memory Read

EVRS 75_{/100} Urgent priority	CVSS V3.1 7.5 High · NVD	EPSS 0.576 99.09th percentile · FIRST	CISA DEADLINE Feb 7, 2024 KEV since 2024 · 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	On the CISA KEV catalog for over two years
☒ EPSS	0.576 probability	☐ Pre-patch disclosure	Disclosure status unavailable
☒ CVSS	Base score 7.5	☐ Microsoft Exploitability Index	Not a Microsoft CVE

Remediation

Patch This Cycle Patch or fixed version identified

CISA required action: Apply mitigations per vendor instructions 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	≥ 12.1 < 12.1-55.302 ≥ 13.0 < 13.0-92.21 ≥ 13.1 < 13.1-37.176 ≥ 13.1 < 13.1-51.15 ≥ 14.1 < 14.1-12.35	12.1-55.302 · 13.0-92.21 · 13.1-37.176 · 13.1-51.15 · 14.1-12.35	NVD
netScaler gateway	≥ 13.0 < 13.0-92.21 ≥ 13.1 < 13.1-51.15 ≥ 14.1 < 14.1-12.35	13.0-92.21	NVD

Sources

Vendor guidance github.com/advisories/GHSA-8fxh-p33g-qf5m

Additional guidance support.citrix.com/article/CTX584986/netscaler-adc-and-netscaler-gateway-security-bulletin-for-cve20236548-and-cve20236549

NVD nvd.nist.gov/vuln/detail/CVE-2023-6549

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

ENISA EUVD euvd.enisa.europa.eu/vulnerability/EUVD-2023-58779

Current data evulnable.com/vulnerability-management/cve/CVE-2023-6549

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