

CVE-2026-3055

Citrix NetScaler Out-of-Bounds Read Vulnerability

CISA KEV since Mar 30, 2026

Actively exploited

Public exploit module (Metasploit)

Insufficient input validation in NetScaler ADC and NetScaler Gateway when configured as a SAML IDP leading to memory overread

EVRS 75/₁₀₀ Urgent priority	CVSS V4.0 9.3 Critical · NVD	EPSS 0.040 90.6th percentile · FIRST	CISA DEADLINE Apr 2, 2026 CISA federal deadline · Overdue by 7 months
---	--	--	---

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 year
☒ EPSS	0.040 probability	☐ Pre-patch disclosure	Disclosure status unavailable
☒ CVSS	Base score 9.3	☐ 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	≥ 13.1 < 13.1-37.262 ≥ 13.1 < 13.1-62.23 ≥ 14.1 < 14.1-60.58	13.1-37.262 · 13.1-62.23 · 14.1-60.58	NVD
netscaler gateway	≥ 13.1 < 13.1-62.23 ≥ 14.1 < 14.1-60.58	13.1-62.23 · 14.1-60.58	NVD

Sources

Vendor guidance	github.com/advisories/GHSA-wv7p-q4p2-p6pf	Additional guidance	support.citrix.com/support-home/kbsearch/article?articleNumber=CTX696300
support.citrix.com	support.citrix.com/support-home/kbsearch/article?articleNumber=CTX696300&articleURL=NetScaler_ADC_and_NetScaler_Gateway_Security_Bulletin_for_CVE_2026_3055_and_CVE_2026_4368	NVD	nvd.nist.gov/vuln/detail/CVE-2026-3055
CISA KEV	cisa.gov/known-exploited-vulnerabilities-catalog	ENISA EUVD	euvd.enisa.europa.eu/vulnerability/EUVD-2026-14546
Current data	evulnable.com/vulnerability-management/cve/CVE-2026-3055		

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