Insufficient input validation leading to memory overread

MITRE | NVD | CVE.ORG | Print: PDF

Summary

CVE	CVE-2026-3055
State	PUBLISHED
Assigner	NetScaler
Source Priority	CVE Program / NVD first with legacy fallback
Published	2026-03-23 21:17:17 UTC
Updated	2026-03-31 13:18:14 UTC
Description	Insufficient input validation in NetScaler ADC and NetScaler Gateway when configured as a SAML IDP leading to memory

Risk And Classification

Primary CVSS: v4.0 9.3 CRITICAL from 50a63c94-1ea7-4568-8c11-eb79e7c5a2b5

CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:H/VI:H/VA:H/SC:L/SI:L/SA:L/E:X/CR:X/IR:X/AR:X/MAV:X/MAC:X/MAT:X/MPR:X/MUI:X/MVC:X/MVI:X/MVA:X/MSC:X/MSI:X/MSA:X/S:X/AU:X/R:X/V:X/RE:X/U:X

EPSS: 0.443010000 probability, percentile 0.975320000 (date 2026-04-01)

CISA KEV: Listed on 2026-03-30; due 2026-04-02; ransomware use Unknown

Problem Types: CWE-125 | CWE-125 CWE-125 Out-of-bounds Read

Version	Source	Type	Score	Severity	Vector
4.0	50a63c94-1ea7-4568-8c11-eb79e7c5a2b5	Secondary	9.3	CRITICAL	CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:H/VI:H/V
4.0	CNA	CVSS	9.3	CRITICAL	CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:H/VI:H/V
3.1	nvd@nist.gov	Primary	9.8	CRITICAL	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

CVSS v4.0 Breakdown

Attack Vector

Network

Attack Complexity

Low

Attack Requirements

None

Privileges Required

None

User Interaction

None

Confidentiality

High

Integrity

High

Availability

High

Sub Conf.

Low

Sub Integrity

Low

Sub Availability

Low

CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:H/VI:H/VA:H/SC:L/SI:L/SA:L/E:X/CR:X/IR:X/AR:X/MAV:X/MAC:X/MAT:X/MPR:X/MUI:X/MVC:X/MVI:X/MVA:X/MSC:X/MSI:X/MSA:X/S:X/AU:X/R:X/V:X/RE:X/U:X

CVSS v3.1 Breakdown

Attack Vector

Network

Attack Complexity

Low

Privileges Required

None

User Interaction

None

Scope

Unchanged

Confidentiality

High

Integrity

High

Availability

High

CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

CISA Known Exploited Vulnerability

Vendor	Citrix
Product	NetScaler
Name	Citrix NetScaler Out-of-Bounds Read Vulnerability
Required Action	Apply mitigations per vendor instructions, follow applicable BOD 22-01 guidance for cloud services, or discontinue use of the prod are unavailable.

Notes	https://support.citrix.com/support-home/kbsearch/article?articleNumber=CTX696300&articleURL=NetScaler_ADC_and_NetScaler_Gateway_Security_Bulletin_for_CVE_2026_3055_and_ ; https://nvd.nist.gov/vuln/detail/CVE-2026-3055

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Citrix	Netscaler Application Delivery Controller	All	All	All	All
Application	Citrix	Netscaler Application Delivery Controller	All	All	All	All
Application	Citrix	Netscaler Application Delivery Controller	All	All	All	All

Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	NetScaler	ADC	affected 14.1 66.59 patch	Not specified
CNA	NetScaler	ADC	affected 13.1 62.23 patch	Not specified
CNA	NetScaler	ADC	affected 13.1 FIPS and NDcPP 37.262 patch	Not specified
CNA	NetScaler	Gateway	affected 14.1 66.59 patch	Not specified
CNA	NetScaler	Gateway	affected 13.1 62.23 patch	Not specified

References

Reference	Source	Link
labs.watchtowr.com/please-we-beg-just-one-weekend-free-of-appliances-citrix-nets...	134c704f-9b21-4f2e-91b3-4a467353bcc0	labs.wat
support.citrix.com/support-home/kbsearch/article	50a63c94-1ea7-4568-8c11-eb79e7c5a2b5	support.
www.cisa.gov/known-exploited-vulnerabilities-catalog	134c704f-9b21-4f2e-91b3-4a467353bcc0	www.cis
CVE Program record	CVE.ORG	www.cve
NVD vulnerability detail	NVD	nvd.nist.
CISA Known Exploited Vulnerabilities catalog	CISA	www.cis

No vendor comments have been submitted for this CVE.

Additional Advisory Data

Source	Time	Event
ADP	2026-03-30T00:00:00.000Z	CVE-2026-3055 added to CISA KEV

There are currently no legacy QID mappings associated with this CVE.

CVE.report and Source URL Uptime Status status.cve.report