

CVE-2019-12991

Citrix SD-WAN and NetScaler Command Injection Vulnerability

CISA KEV since Mar 25, 2022

Actively exploited

Citrix SD-WAN 10.2.x before 10.2.3 and NetScaler SD-WAN 10.0.x before 10.0.8 have Improper Input Validation (issue 5 of 6).

EVRS 79 / ₁₀₀ Urgent priority	CVSS V3.1 8.8 High · NVD	EPSS 0.745 99.5th percentile · FIRST	CISA DEADLINE Apr 15, 2022 KEV since 2022 · 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	0.745 probability	☐ Pre-patch disclosure	Disclosure status unavailable
☒ CVSS	Base score 8.8	☐ Microsoft Exploitability Index	Not a Microsoft CVE

Remediation

Patch This Cycle Patch or fixed version identified

CISA required action: Apply updates per vendor instructions.

Basis: CISA KEV required action

Affected and fixed versions

PACKAGE	AFFECTED	FIXED IN	SOURCE
netscaler sd-wan	≥ 10.0.0 < 10.0.8	10.0.8	NVD
sd-wan	≥ 10.2.0 < 10.2.3	10.2.3	NVD

Sources

Vendor guidance github.com/advisories/GHSA-462p-6gjj-6wj6
NVD nvd.nist.gov/vuln/detail/CVE-2019-12991

ENISA EUVD euvd.enisa.europa.eu/vulnerability/EUVD-2019-4566

Additional guidance support.citrix.com/article/CTX251987
CISA KEV cisa.gov/known-exploited-vulnerabilities-catalog
Current data evulnable.com/vulnerability-management/cve/CVE-2019-12991

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