

CVE-2026-59310

Broadcom VMware vCenter Path Traversal Vulnerability

Exigent

CISA KEV since Aug 18, 2026

Actively exploited

Ransomware use known

VMware vCenter contains a directory traversal vulnerability in the Syslog server. A malicious actor with network access to vCenter may exploit this issue to execute arbitrary code.

EVRS 85 /100 Immediate priority	CVSS V3.1 9.8 Critical · NVD	EPSS 0.026 85th percentile · FIRST	CISA DEADLINE Aug 21, 2026 CISA federal deadline · Overdue by 2 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	Known ransomware campaigns	☒ KEV recency	Added to CISA KEV within the last 90 days
☒ EPSS	0.026 probability	☐ Pre-patch disclosure	Disclosure status unavailable
☒ CVSS	Base score 9.8	☐ Microsoft Exploitability Index	Not a Microsoft CVE

Remediation

Out-of-band / urgent Patch or fixed version identified

CISA required action: Apply mitigations in accordance with vendor instructions, ensuring compliance with CISA's BOD 26-04 Prioritizing Security Updates Based on Risk (see URL in Notes) guidance and CISA's "Forensics Triage Requirements" (see URL in Notes). Follow applicable BOD 26-04 guidance for cloud services or discontinue use of the product if mitigations are unavailable. Stakeholders are responsible for evaluating each asset's internet exposure and ensuring adherence to BOD 26-04 patching guidelines.

Basis: CISA KEV required action

Affected and fixed versions

PACKAGE	AFFECTED	FIXED IN	SOURCE
vcenter server	< 8.0 8.0 ≥ 9.0 < 9.0.2.0100 ≥ 9.1 < 9.1.0.0300	8.0 · 9.0.2.0100 · 9.1.0.0300	NVD
telco cloud infrastructure	3.0	no fixed version listed	NVD
telco cloud platform	≥ 3.0 ≤ 5.2	no fixed version listed	NVD
cloud foundation	—	no fixed version listed	NVD
vsphere foundation	—	no fixed version listed	NVD

Sources

Vendor guidance	github.com/advisories/GHSA-v2gp-49gj-2c9f	support.broadcom.com	support.broadcom.com/web/ecx/support-content-notification/-/external/content/SecurityAdvisories/0/38017
BOD 26-04	cisa.gov/news-events/directives/bod-26-04-prioritizing-security-updates-based-risk	Forensics Triage Requirements	cisa.gov/news-events/directives/bod-26-04-implementation-guidance-prioritizing-security-updates-based-risk
NVD	nvd.nist.gov/vuln/detail/CVE-2026-59310	CISA KEV	cisa.gov/known-exploited-vulnerabilities-catalog
ENISA EUVD	euvd.enisa.europa.eu/vulnerability/EUVD-2026-51097	Current data	evulnable.com/vulnerability-management/cve/CVE-2026-59310

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