

CVE-2025-22226

VMware ESXi, Workstation, and Fusion Information Disclosure Vulnerability

CISA KEV since Mar 4, 2025

Actively exploited

VMware ESXi, Workstation, and Fusion contain an information disclosure vulnerability due to an out-of-bounds read in HGFS. A malicious actor with administrative privileges to a virtual machine may be able to exploit this issue to leak memory from the vmx process.

EVRS 75/₁₀₀ Urgent priority	CVSS V3.1 6.0 Medium · NVD	EPSS 0.018 78th percentile · FIRST	CISA DEADLINE Mar 25, 2025 KEV since 2025 · 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	Added to CISA KEV within the last two years
☒ EPSS	0.018 probability	☐ Pre-patch disclosure	Disclosure status unavailable
☒ CVSS	Base score 6.0	☐ 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
cloud foundation	–	no fixed version listed	NVD
fusion	≥ 13.0.0 < 13.6.3	13.6.3	NVD
telco cloud infrastructure	2.2 2.5 2.7 3.0	no fixed version listed	NVD
telco cloud platform	2.0 2.5 2.7 3.0 4.0 4.0.1 5.0	no fixed version listed	NVD
workstation	≥ 17.0 < 17.6.3	17.6.3	NVD
esxi	7.0 8.0	no fixed version listed	NVD



Sources

Vendor guidance	github.com/advisories/GHSA-37f6-vjg7-8c6c	Additional guidance	support.broadcom.com/web/ecx/support-content-notification/-/external/content/SecurityAdvisories/0/25390
NVD	nvd.nist.gov/vuln/detail/CVE-2025-22226	CISA KEV	cisa.gov/known-exploited-vulnerabilities-catalog
ENISA EUVD	euvd.enisa.europa.eu/vulnerability/EUVD-2025-7605	Current data	evulnable.com/vulnerability-management/cve/CVE-2025-22226

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