

CVE-2024-37085

VMware ESXi Authentication Bypass Vulnerability

CISA KEV since Jul 30, 2024

Actively exploited

Ransomware use known

VMware ESXi contains an authentication bypass vulnerability. A malicious actor with sufficient Active Directory (AD) permissions can gain full access to an ESXi host that was previously configured to use AD for user management <https://blogs.vmware.com/vsphere/2012/09/joining-vsphere-hosts-to-active-directory.html> by re-creating the configured AD group ('ESXi Admins' by default) after it was deleted from AD.

EVRS

75/100

Urgent priority

CVSS V3.1

7.2

High · NVD

EPSS

0.268

98th percentile · FIRST

CISA DEADLINE

Aug 20, 2024

KEV since 2024 · 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	Known ransomware campaigns	☐ KEV recency	On the CISA KEV catalog for over two years
☒ EPSS	0.268 probability	☐ Pre-patch disclosure	Disclosure status unavailable
☒ CVSS	Base score 7.2	☐ Microsoft Exploitability Index	Not a Microsoft CVE

Remediation

Patch This Cycle Patch or fixed version identified**CISA required action:** Apply mitigations per vendor instructions 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	≥ 4.0 < 5.2	5.2	NVD
esxi	7.0 8.0	no fixed version listed	NVD

Sources

Vendor guidance	support.broadcom.com/web/ecx/support-content-notification/-/external/content/SecurityAdvisories/0/24505	NVD	nvd.nist.gov/vuln/detail/CVE-2024-37085
CISA KEV	cisa.gov/known-exploited-vulnerabilities-catalog	ENISA EUVD	euvd.enisa.europa.eu/vulnerability/EUVD-2024-36416
Current data	evulnable.com/vulnerability-management/cve/CVE-2024-37085		

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