

CVE-2020-3950

VMware Multiple Products Privilege Escalation Vulnerability

CISA KEV since Nov 3, 2021

Actively exploited

Public exploit module (Metasploit)

VMware Fusion (11.x before 11.5.2), VMware Remote Console for Mac (11.x and prior before 11.0.1) and Horizon Client for Mac (5.x and prior before 5.4.0) contain a privilege escalation vulnerability due to improper use of setuid binaries. Successful exploitation of this issue may allow attackers with normal user privileges to escalate their privileges to root on the system where Fusion, VMRC or Horizon Client is installed.

EVRS 75/₁₀₀ Urgent priority	CVSS V3.1 7.8 High · NVD	EPSS 0.073 94.3rd percentile · FIRST	CISA DEADLINE May 3, 2022 KEV since 2021 · 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	0.073 probability	☐ Pre-patch disclosure	Disclosure status unavailable
☒ CVSS	Base score 7.8	☐ 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
fusion	≥ 11.0.0 < 11.5.2	11.5.2	NVD
horizon client	≥ 5.0.0 < 5.4.0	5.4.0	NVD
remote console	≥ 11.0.0 < 11.0.1	11.0.1	NVD
macos	—	no fixed version listed	NVD

Sources

Vendor guidance github.com/advisories/GHSA-fx3w-hj7j-hfgf

Additional guidance vmware.com/security/advisories/VMSA-2020-0005.html

NVD nvd.nist.gov/vuln/detail/CVE-2020-3950

CISA KEV cisa.gov/known-exploited-vulnerabilities-catalog

ENISA EUVD euvd.enisa.europa.eu/vulnerability/EUVD-2020-25215

Current data evulnable.com/vulnerability-management/cve/CVE-2020-3950

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