

CVE-2016-3643

SolarWinds Virtualization Manager Privilege Escalation Vulnerability

CISA KEV since Nov 3, 2021

Actively exploited

SolarWinds Virtualization Manager 6.3.1 and earlier allow local users to gain privileges by leveraging a misconfiguration of sudo, as demonstrated by "sudo cat /etc/passwd."

EVRS 75 / ₁₀₀ Urgent priority	CVSS V3.1 7.8 High · NVD	EPSS 0.037 89.6th 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	0.037 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
virtualization manager	≤ 6.3.1	after 6.3.1	NVD

Sources

Vendor guidance	github.com/advisories/GHSA-fww7-75jj-wj62	NVD	nvd.nist.gov/vuln/detail/CVE-2016-3643
CISA KEV	cisa.gov/known-exploited-vulnerabilities-catalog	ENISA EUVD	euvd.enisa.europa.eu/vulnerability/EUVD-2016-4668
Current data	evulnable.com/vulnerability-management/cve/CVE-2016-3643		

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