

CVE-2020-3992

VMware ESXi OpenSLP Use-After-Free Vulnerability

Exigent CISA KEV since Nov 3, 2021 Actively exploited Ransomware use known

OpenSLP as used in VMware ESXi (7.0 before ESXi_7.0.1-0.0.16850804, 6.7 before ESXi670-202010401-SG, 6.5 before ESXi650-202010401-SG) has a use-after-free issue. A malicious actor residing in the management network who has access to port 427 on an ESXi machine may be able to trigger a use-after-free in the OpenSLP service resulting in remote code execution.

EVRS 89/100 Immediate priority	CVSS V3.1 9.8 Critical · NVD	EPSS 0.830 99.68th 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	Known ransomware campaigns	☐ KEV recency	On the CISA KEV catalog for over two years
☒ EPSS	0.830 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 updates per vendor instructions.
 Basis: CISA KEV required action

Affected and fixed versions

PACKAGE	AFFECTED	FIXED IN	SOURCE
cloud foundation	≥ 3.0 < 3.10.1.2 ≥ 4.0 < 4.1.0.1	3.10.1.2 · 4.1.0.1	NVD
esxi	6.5 6.7 7.0.0	no fixed version listed	NVD

Sources

Vendor guidance	vmware.com/security/advisories/VMSA-2020-0023.html	NVD	nvd.nist.gov/vuln/detail/CVE-2020-3992
CISA KEV	cisa.gov/known-exploited-vulnerabilities-catalog	ENISA EUVD	euvd.enisa.europa.eu/vulnerability/EUVD-2020-25257
Current data	evulnable.com/vulnerability-management/cve/CVE-2020-3992		

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