

CVE-2019-5544

VMware ESXi and Horizon DaaS OpenSLP Heap-Based Buffer Overflow Vulnerability

Exigent

CISA KEV since Nov 3, 2021

Actively exploited

Ransomware use known

OpenSLP as used in ESXi and the Horizon DaaS appliances has a heap overwrite issue. VMware has evaluated the severity of this issue to be in the Critical severity range with a maximum CVSSv3 base score of 9.8.

EVRS 93/100 Immediate priority	CVSS V3.1 9.8 Critical · NVD	EPSS 0.981 99.91st 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	0.981 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 · 8 more affected products on the NVD record

PACKAGE	AFFECTED	FIXED IN	SOURCE
horizon daas	≥ 8.0.0 < 9.0.0.0	no fixed version listed	NVD
openslp	≤ 2.0.0	no fixed version listed	NVD
esxi	6.0 6.5 6.7	no fixed version listed	NVD
enterprise linux desktop	6.0 7.0	no fixed version listed	NVD
enterprise linux for ibm z systems	6.0 s390x 7.0 s390x	no fixed version listed	NVD
enterprise linux for ibm z systems eus	7.7 s390x	no fixed version listed	NVD
enterprise linux for power big endian	6.0 ppc64 7.0 ppc64	no fixed version listed	NVD
enterprise linux for power big endian eus	7.7 ppc64	no fixed version listed	NVD

Sources

Vendor guidance github.com/advisories/GHSA-4734-5452-r5fh
NVD nvd.nist.gov/vuln/detail/CVE-2019-5544

Additional guidance access.redhat.com/errata/RHSA-2019:4240
CISA KEV cisa.gov/known-exploited-vulnerabilities-catalog

ENISA EUVD euvd.enisa.europa.eu/vulnerability/EUVD-2019-15119

Current data evulnable.com/vulnerability-management/cve/CVE-2019-5544

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