Security Advisory 2022-001

Important Vulnerability in VMWare

January 6, 2022 — v1.0

TLP:WHITE

History:

- *06/01/2022 — v1.0 – Initial publication*

Summary

On the 4th of January 2022, VMware has released a security alert for a vulnerability affecting VMware Workstation, Fusion, ESXi Server and Cloud Foundation [1]. This vulnerability tracked as CVE-2021-22045 has an important CVSSv3 score of 7.7. A malicious actor with access to a virtual machine with CD-ROM device emulation may be able to exploit a heap overflow vulnerability in conjunction with other issues to execute code on the hypervisor from a virtual machine.

Successful exploitation requires CD image to be attached to the virtual machine.

Technical Details

This is a heap-overflow vulnerability located in CD-ROM device emulation in VMware Workstation, Fusion and ESXi that was privately reported to VMware.

Affected Products

The following products are affected by the vulnerability :

Product	Affected Versions	Platform
VMware ESXi	6.5, 6.7, 7	Any
VMware Workstation	16.x	Any
VMware Fusion	12.x	OS X
VMware Cloud Foundation (ESXi)	3.x, 4.x	Any

All previous releases of VMware ESXi 6.5 and 6.7 are vulnerable.

Recommendations

VMware has released an update and workarounds that fixes the CVE-2021-22045 [2,3,4] and a general workaround [4] showing how to disable CD-ROM/DVD devices on all running virtual machines. The workaround is meant to be a temporary solution until updates documented in [1] can be deployed.

CERT-EU strongly recommends patching as per the table below:

Product	Fixed Version	Workaround
VMware ESXi 6.5	ESXi650-202111101-SG	6.5 P07 Build number 18678235 [2] as per [4]
VMware ESXi 6.7	ESXi670-202110101-SG	6.7 P06 Build Number 18828794 [3] as per [4]
VMware ESXi 7	Pending	[4]
VMware Workstation 16.x	16.2.0	[5]
VMware Fusion 12.x	12.2.0	[5]
VMware Cloud Foundation (ESXi) 3.x, 4.x	Pending	[4]

There is no requirement to implement the workaround once the recommended upgrade is complete.

References

[1] https://www.vmware.com/security/advisories/VMSA-2022-0001.html

[2] https://docs.vmware.com/en/VMware-vSphere/6.5/rn/esxi650-202110001.html

[3] https://docs.vmware.com/en/VMware-vSphere/6.7/rn/esxi670-202111001.html

[4] https://kb.vmware.com/s/article/87249

[5] https://kb.vmware.com/s/article/87206