Hive Pro

THREAT ADVISORY

High severity vulnerability in VMware Workstation, Fusion, and ESXi

TA2022003

Threat Level AMBER

Publish Date – Jan 6, 2022

A heap buffer overflow vulnerability has been discovered in multiple products of VMware. This bug has been tracked as CVE-2021-22045, if exploited would result in execution of arbitrary code by the attacker.

Heap overflows are memory concerns that can cause data corruption or unexpected behavior in any process that accesses the affected memory space - in some situations leading in remote code execution (RCE).

The bug affects ESXi versions 6.5, 6.7, 7.0; Workstation version 16.x; Fusion version 12.x and Cloud Foundation versions 4.x, 3.x.

Organizations can patch some of the versions from the link below. However, some of them still awaits patches and organizations can use these steps to mitigate the flaw:
1) Log in to a vCenter Server system using the vSphere Web Client.
2) Right-click the virtual machine and click Edit Settings.
3) Select the CD/DVD drive and uncheck "Connected" and "Connect at power on" and remove any attached ISOs.

According to the vendor, users can execute the following command to enumerate the VMs that have a CD-ROM/DVD drive attached:
Get-VM | Get-CDDrive | Where {$_.extensiondata.connectable.connected -eq $true} | Select Parent

The attached CD-ROM/DVD device will then be removed and disconnected using the following command:
Get-VM | Get-CDDrive | Where {$_.extensiondata.connectable.connected -eq $true} | Set-CDDrive -NoMedia -confirm:$false

Vulnerability Details

CVE ID	Affected Products	Affected CPE	Vulnerability Name	CWE ID
CVE-2021-22045	VMware ESXi versions 6.5, 6.7, 7.0; VMware Workstation version 16.x; VMware Fusion version 12.x; VMware Cloud Foundation versions 4.x, 3.x	cpe:2.3:a:vmware:esxi:*:*:*:*:*:*:*:*, cpe:2.3:a:vmware:fusion:*:*:*:*:*:*:*:*, cpe:2.3:a:vmware:workstation:*:*:*:*:*:*:*:*, cpe:2.3:a:vmware:cloud_foundation:-:*:*:*:*:*:*:*	VMware Workstation, Fusion and ESXi buffer overflow	CWE-122

Patch Links

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

References

https://www.cisa.gov/uscert/ncas/current-activity/2022/01/05/vmware-releases-security-updates
https://thehackernews.com/2022/01/vmware-patches-important-bug-affecting.html
https://threatpost.com/unpatched-vmware-bug-hypervisor-takeover/177428/