CERT-EU
FOR THE EU INSTITUTIONS, BODIES AND AGENCIES

Security Advisory 2020-057

Critical Vulnerabilities in VMware Products

November 25, 2020 — v1.0

TLP:WHITE

History:

- *25/11/2020 — v1.0 – Initial publication*

Summary

VMware has released security advisories to address several security vulnerabilities including critical ones [1, 2]. Patches or workarounds are available for some of these vulnerabilities.

Technical Details

CVE-2020-4004 (CVSS Score: Base 9.3)

Critical vulnerability, described as a *Use-after-free vulnerability in XHCI USB controller*.

A malicious actor with local administrative privileges on a virtual machine may exploit this issue to execute code as the virtual machine's VMX process running on the host. The VMX process runs in the VMkernel and is responsible for handling I/O to devices. As such data exfiltration would be possible [3, 4].

CVE-2020-4005 (CVSS Score: Base 8.8)

Is a VMX elevation-of-privilege vulnerability. A malicious actor with privileges within the VMX process only, may escalate their privileges on the affected system. Successful exploitation of this issue is only possible when chained with another vulnerability (e.g. CVE-2020-4004) [1, 3].

CVE-2020-4006 (CVSS Score: Base 9.1)

A critical unpatched command injection vulnerability affects VMware products. A malicious actor with network access to the administrative configurator on port 8443 and a valid password for the configurator admin account can execute commands with unrestricted privileges on the underlying operating system [2].

Affected Products

These vulnerabilities affect several products as follow:

CVE-2020-4004

- VMware ESXi 7.0 before ESXi70U1b-17168206,
- VMware ESXi 6.7 before ESXi670-202011101-SG,
- VMware ESXi 6.5 before ESXi650-202011301-SG,
- Workstation 15.x before 15.5.7,
- Fusion 11.x before 11.5.7.

CVE-2020-4005

- VMware ESXi 7.0 before ESXi70U1b-17168206,
- VMware ESXi 6.7 before ESXi670-202011101-SG,
- VMware ESXi 6.5 before ESXi650-202011301-SG.

CVE-2020-4006

- VMware Workspace One Access,
- Access Connector,
- Identity Manager and Identity Manager Connector address.

Recommendations

VMware has released software updates that address CVE-2020-4004 and CVE-2020-4005. To remediate apply the patches listed in [1]. Workarounds for CVE-2020-4004 have been listed also on [1].

Patches for CVE-2020-4006 are forthcoming. In the meantime workarounds for CVE-2020-4006 have been published [2].

References

[1] https://www.vmware.com/security/advisories/VMSA-2020-0026.html

[2] https://www.vmware.com/security/advisories/VMSA-2020-0027.html

[3] https://www.theregister.com/2020/11/20/vmware_esxi_flaws/

[4] https://nvd.nist.gov/vuln/detail/CVE-2020-4004

[5] https://nvd.nist.gov/vuln/detail/CVE-2020-4005

[6] https://nvd.nist.gov/vuln/detail/CVE-2020-4006