CERT-EU
FOR THE EU INSTITUTIONS, BODIES AND AGENCIES

Security Advisory 2020-015

Critical Vulnerability in VMWare Products

March 13, 2020 — v1.0

TLP:WHITE

History:

- *13/03/2020 — v1.0 – Initial publication*

Summary

On the 12th of March 2020, VMWare released an advisory concerning three vulnerabilities in VMWare products [1]. The most critical one (CVE-2020-3947) could be exploited by an attacker to execute code on a host system from a malicious or compromised guest.

It is strongly recommended to update **VMWare Workstation** and **VMWare Fusion**, especially for security analysts running malware in Virtual Machines for analysis.

Technical Details

The vulnerability CVE-2020-3947 with **critical severity** (CVSSv3 score of 9.3) is due to a *use-after-free* vulnerability in `vmnetdhcp` (VMware VMnet DHCP service). VMware VMnet DHCP service is used by the Virtual Network Editor in VMWare.

The vulnerability CVE-2020-3948 with **important severity** (CVSSv3 score of 7.8) concern a local privilege escalation vulnerability on Linux Guest VMs due to improper file permissions in Cortado Thinprint. Exploitation is only possible if VMware Tools is installed in the VM (which are installed by default on Workstation and Fusion).

The vulnerability CVE-2019-5543 with **important severity** (CVSSv3 score of 7.3) concerns the folder containing configuration files for the VMware USB arbitration service that was found to be writable by all users in VMware Horizon Client for Windows, VMRC for Windows and Workstation for Windows.

Products Affected

Products affected by the critical severity vulnerability:

- VMWare Workstation 15.x before 15.5.2
- VMWare Fusion 11.x before 11.5.2

Products affected by the important severity vulnerability:

- Horizon Client for Windows 5.x before 5.3.0 and prior versions
- VMRC for Windows 10.x

Recommendations

Update VMWare products to the latest versions:

- VMWare Workstation 15.5.2
- VMWare Fusion 11.5.2
- Horizon Client for Windows 5.3.0

References

[1] https://www.vmware.com/security/advisories/VMSA-2020-0004.html