CERT-EU
FOR THE EU INSTITUTIONS, BODIES AND AGENCIES

Security Advisory 2019-008

VMware ESXi, Workstation, and Fusion Multiple Security Vulnerabilities

April 02, 2019 — v1.0

TLP:WHITE

History:

- *02/04/2019 — v1.0 – Initial publication*

Summary

VMware has released security updates [1] to address security vulnerabilities in multiple products. An attacker could exploit some of these vulnerabilities to take control of an affected system including allowing the guest to execute code on the host system.

Technical Details

- **VMware ESXi, Workstation and Fusion UHCI Out-of-Bounds Read/Write (CVE-2019-5518) and TOCTOU (CVE-2019-5519) Vulnerabilities**

VMware ESXi, Workstation and Fusion contain an out-of-bounds read/write vulnerability and a Time-of-check Time-of-use (TOCTOU) vulnerability in the virtual USB 1.1 UHCI (Universal Host Controller Interface). Exploitation of these issues requires an attacker to have access to a virtual machine with a virtual USB controller present. These issues may allow a guest to execute code on the host.

- **VMware Workstation and Fusion Out-of-Bounds Write Vulnerability in `e1000` Virtual Network Adapter (CVE-2019-5524)**

VMware Workstation and Fusion contain an out-of-bounds write vulnerability in the `e1000` virtual network adapter. This issue may allow a guest to execute code on the host.

- **VMware Workstation and Fusion Out-of-Bounds Write Vulnerability in `e1000` and `e1000e` Virtual Network Adapters (CVE-2019-5515)**

VMware Workstation and Fusion updates address an out-of-bounds write vulnerability in the `e1000` and `e1000e` virtual network adapters. Exploitation of this issue may lead to code execution on the host from the guest, but it is more likely to result in a denial-of-service of the guest.

- **VMware Fusion Unauthenticated APIs Security Vulnerability (CVE-2019-5514)**

VMware Fusion contains a security vulnerability due to certain unauthenticated APIs accessible through a web socket. An attacker may exploit this issue by tricking the host user to execute a JavaScript to perform unauthorized functions on the guest machine where VMware Tools are installed. This may further be exploited to execute commands on the guest machines.

Products Affected

VMware Product	CVE-2019-5518	CVE-2019-5519	CVE-2019-5524	CVE-2019-5515	CVE-2019-5514
ESXi 6.7	Affected	Affected	-	-	-
ESXi 6.5	Affected	Affected	-	-	-
ESXi 6.0	Affected	Affected	-	-	-
Workstation 15.x	Affected	Affected	-	Affected	-
Workstation 14.x	Affected	Affected	Affected	Affected	-
Fusion 11.x	Affected	Affected	-	Affected	Affected
Fusion 10.x	Affected	Affected	Affected	Affected	-

Recommendations

VMWare has released a patch for affected products [1–5]. Upgrade affected products to the following versions:

VMware Product	Replace with/ Apply Patch
ESXi 6.7	ESXi670-201903001
ESXi 6.5	ESXi650-201903001
ESXi 6.0	ESXi600-201903001
Workstation 15.x	15.0.4
Workstation 14.x	14.1.7
Fusion 11.x	11.0.3
Fusion 10.x	10.1.6

References

[1] https://www.vmware.com/be/security/advisories/VMSA-2019-0005.html

[2] https://my.vmware.com/group/vmware/patch

[3] https://www.vmware.com/go/downloadworkstation

[4] https://www.vmware.com/go/downloadplayer

[5] https://www.vmware.com/go/downloadfusion