CERT-EU Security Advisory 2017-007

Critical Vulnerabilities in VMWare ESXi, Workstation, and Fusion

March 31, 2017 — v1.1

History:

- *29/03/2017 — v1.0: Initial publication*
- *31/03/2017 — v1.1: Correction regarding VMWare ESXi 5.5*

Summary

On March 28, 2017, VMWare released an advisory for VMWare ESXi, Workstation, and Fusion products [1]. The advisory addresses critical and moderate security issues.

Critical vulnerabilities may allow a guest system to execute code on the host system (CVE-2017-4902, CVE-2017-4903, and CVE-2017-4904).

The other vulnerability (CVE-2017-4905) may lead to information leak from the guest system.

These vulnerabilities were discovered by two teams (Team Sniper and Qihoo 360) during Pwn2Own event at CanSecWest [2].

Technical Details

The discovered vulnerabilities targeting VMWare products are:

- CVE-2017-4902 (critical): Heap overflow leading to arbitrary code execution
- CVE-2017-4903 (critical): Uninitialized stack value leading to arbitrary code execution
- CVE-2017-4904 (critical): Uninitialized stack value leading to arbitrary code execution
- CVE-2017-4905 (moderate): Uninitialized memory read leading to information disclosure

Vulnerable Systems

- VMWare ESXi 5.5 - CVE-2017-4904 (moderate) and CVE-2017-4905 (moderate)
- VMWare ESXi 6.0 - all vulnerabilities except CVE-2017-4902
- VMWare ESXi 6.5 - all vulnerabilities
- VMware Workstation 12.X - all vulnerabilities
- VMware Fusion 8.x (OS X) - all vulnerabilities

Note: VMware ESXi 6.0 is not affected by CVE-2017-4902. Furthermore, CVE-2017-4904 only leads to denial of service on VMWare ESXi 5.5 (moderate).

Recommendations

Apply upgrades provided by VMWare for all affected products as soon as possible [1].

No other workarounds are available.

References

[1] https://www.vmware.com/security/advisories/VMSA-2017-0006.html

[2] https://blogs.vmware.com/security/2017/03/security-landscape-pwn2own-2017.html