CERT-EU Security Advisory 2017-027

Multiple Security Vulnerabilities Affecting VMware Products

December 22, 2017 — v1.0

History:

- *22/12/2017 — v1.0: Initial publication*

Summary

On the 19th of December 2017, VMware released updates to address multiple security vulnerabilities in ESXi, vCenter Server Appliance, Workstation and Fusion [1]. The most serious of the vulnerabilities could allow remote arbitrary code execution in a virtual machine.

Technical Details

The vulnerabilities received four CVEs: CVE-2017-4941, CVE-2017-4933, CVE-2017-4940, and CVE-2017-4943.

The first vulnerability (CVE-2017-4941) can be exploited by a remote attacker to execute code in a virtual machine via an authenticated Virtual Network Computing (VNC) session. According to Cisco Talos *A specially crafted set of VNC packets can cause a type confusion resulting in stack overwrite, which could lead to code execution* [2]. ESXi, Workstation and Fusion are affected [1].

The second vulnerability (CVE-2017-4933) allows an attacker to execute arbitrary code in a virtual machine using specially crafted VNC packets. In that case *A specially crafted set of VNC packets can cause a heap overflow resulting in heap corruption* [3]. ESXi, Workstation and Fusion are affected [1].

The third vulnerability (CVE-2017-4940) allows for persistent cross-site scripting (XSS) in ESXi Host Client. It could be exploited by injecting Javascript code that gets executed by other users [1].

Last vulnerability is (CVE-2017-4943) is a privilege escalation affecting VMware vCenter Server Appliance `showlog` plugin. It can be exploited by an attacker with low privileges to gain root level access [1].

Products Affected

Several versions and components of VMware ESXi, vCenter Server Appliance, Workstation and Fusion are affected [1].

Recommendations

- Review the patch level for your product and version and update accordingly [1].
- As a workaround for CVE-2017-4941 and CVE-2017-4933 vulnerabilities: Exploitation can be blocked by disabling VNC in `.vmx` configuration of VMS and blocking the traffic on firewall.

References

[1] https://www.vmware.com/security/advisories/VMSA-2017-0021.html

[2] https://www.talosintelligence.com/reports/TALOS-2017-0369

[3] https://www.talosintelligence.com/reports/TALOS-2017-0368