CERT-EU
FOR THE EU INSTITUTIONS, BODIES AND AGENCIES

Security Advisory 2021-011

Critical Vulnerabilities in VMware

February 25, 2021 — v1.1

TLP:WHITE

History:

- 24/02/2021 — v1.0 – Initial publication
- 25/02/2021 — v1.1 – Updated with information on PoC available

Summary

On 24th of February 2021, VMware has released a security advisory [1] to address multiple vulnerabilities including a **critical (CVSS Score 9.8) remote code execution (RCE) vulnerability** in the vCenter Server management platform. The vulnerabilities may allow attackers to potentially take control of affected systems. Updates are available to remediate these vulnerabilities in affected VMware products.

On the same day, PT Swarm published an article covering more technical details and the proof-of-concept (PoC) for the RCE vulnerability [4]. The availability of the PoC indicates that wide spread exploitation of this vulnerability may start very soon. **Immediate patching is strongly advised!**

Technical Details

CVE-2021-21972 (CVSS Score: Base 9.8)

This vulnerability, described as a *Remote code execution vulnerability in the vSphere Client*, was reported by Mikhail Klyuchnikov of Positive Technologies, and it can be exploited remotely by unauthenticated attackers in low complexity attacks that do not require user interaction.

The vSphere Client (HTML5) contains a remote code execution vulnerability in a vCenter Server plugin that allows a malicious actor with network access to port 443 to execute commands with unrestricted privileges on the underlying operating system that hosts vCenter Server. The impacted vCenter Server plugin for **vRealize Operations* (vROps) is present in all default installations, with vROPs not being required for the affected endpoint to be available.

As presented in the PoC by PT Swarm, in addition to getting access to the command line, an attacker can perform other malicious actions due to the lack of authentication in the vROps plugin.

CVE-2021-21974 (CVSS Score: Base 8.8)

Critical vulnerability, described as an *ESXi OpenSLP heap-overflow vulnerability*.

OpenSLP as used in ESXi has a heap-overflow vulnerability that may enable attackers residing within the same network segment as ESXi and with access to port 427 to execute arbitrary code remotely on impacted devices. Per the Security Configuration Guides for VMware vSphere, VMware now recommends disabling the OpenSLP service in ESXi if it is not used [2].

Affected Products

These vulnerabilities affect several products as follows:

CVE-2021-21972

- vCenter Server 3.x and 4.x

CVE-2021-21974

- Cloud Foundation (ESXi) 3.x and 4.x

Recommendations

VMware has released software updates that address CVE-2021-21972 and CVE-2021-21974. To remediate – apply the patches listed in [1]. Workarounds for those who cannot immediately update have been listed also in [1].

For the CVE-2021-21974, VMware released also a guideline [3] that documents steps to consume ESXi hot patch asynchronously on top of latest VMware Cloud Foundation (VCF) supported ESXi build.

Due to this security vulnerability's critical nature, and since a PoC has been already released, it is strongly recommended to **update the vulnerable products as soon as possible**!

References

[1] https://www.vmware.com/security/advisories/VMSA-2021-0002.html

[2] https://blogs.vmware.com/vsphere/2021/02/evolving-the-vmware-vsphere-security-configuration-guides.html

[3] https://kb.vmware.com/s/article/82705

[4] https://swarm.ptsecurity.com/unauth-rce-vmware/