CERT-EU
FOR THE EU INSTITUTIONS, BODIES AND AGENCIES

Security Advisory 2021-025

Critical Vulnerability in VMWare vCenter Server

June 7, 2021 — v1.1

TLP:WHITE

History:

- *26/05/2021 — v1.0 – Initial publication*
- *07/06/2021 — v1.1 – Update after PoC release*

Summary

On the 25th of May 2021, VMware has revealed two vulnerabilities in vSphere Client (HTML5) with the updates to address these vulnerabilities [1]. One of the vulnerabilities (CVE-2021-21985) has a critical CVSSv3 score. It may allow an attacker to execute command with unrestricted privileges on the operating system that hosts vCenter Server.

As of the beginning of June, 2021, a proof-of-concept of a RCE exploit targeting the critical vulnerability has been published. This indicates imminent exploitation of this vulnerability in the wild.

Technical Details

The vulnerability tracked as CVE-2021-21985 was reported initially by Ricter Z. from 360 Noah Lab, and it can be remotely exploited by unauthenticated attackers in low complexity attacks which do not require user interaction [7].

A malicious actor with network access on port 443 of the vCenter Server appliances may execute command remotely with unrestricted privileges on the underlying host. This is due to a lack of input validation in the Virtual SAN Health Check plug-in, which is enabled by default. The severity of this issue has been evaluated with CVSSv3 score of 9.8 by VMware [1]. Additional information has also been provided by VMWare in [6].

At the beginning of June, Security Researchers have developed and published a proof-of-concept of a RCE exploit targeting CVE-2021-21985. Moreover, threat intelligence company has monitored attackers scanning actively for Internet-exposed VMware vCenter servers unpatched interface. According to Shodan, thousands of vCenter servers are still reachable from the Internet and may be vulnerable to CVE-2021-21985 [8].

Affected Products

The following products are affected by the vulnerabilities :

Product	Affected Versions	Platform
vCenter Server 7.0	vCenter Server 7.0 Update 2a and earlier	Any
vCenter Server 6.7	vCenter Server 6.7 Update 3m and earlier	Any
vCenter Server 6.5	vCenter Server 6.5 Update 3n and earlier	Any

Recommendations

VMware has released updates that fixes the two vulnerabilities CVE-2021-21985 and CVE-2021-21986 [2, 3, 4] and a workaround [5] showing how to disable VMware plugins in vCenter Server.

CERT-EU strongly recommends patching vCenter Server to the fixed version of the table below:

Product	Fixed Version
vCenter Server 7.0	7.0 U2b
vCenter Server 6.7	6.7 U3n
vCenter Server 6.5	6.5 U3p

References

[1] https://www.vmware.com/security/advisories/VMSA-2021-0010.html

[2] https://docs.vmware.com/en/VMware-vSphere/7.0/rn/vsphere-vcenter-server-70u2b-release-notes.html

[3] https://docs.vmware.com/en/VMware-vSphere/6.7/rn/vsphere-vcenter-server-67u3n-release-notes.html

[4] https://docs.vmware.com/en/VMware-vSphere/6.5/rn/vsphere-vcenter-server-65u3p-release-notes.html

[5] https://kb.vmware.com/s/article/83829

[6] https://blogs.vmware.com/vsphere/2021/05/vmsa-2021-0010.html

[7] https://www.bleepingcomputer.com/news/security/vmware-warns-of-critical-bug-affecting-all-vcenter-server-installs/

[8] https://www.bleepingcomputer.com/news/security/attackers-are-scanning-for-vulnerable-vmware-servers-patch-now/