FOR THE EU INSTITUTIONS, BODIES AND AGENCIES

Security Advisory 2021-052

Critical Vulnerabilities in VMware Products

September 28, 2021 — v1.1

TLP:WHITE

History:

- *22/09/2021 — v1.0 – Initial publication*
- *28/09/2021 — v1.1 – Update with information about the active exploitation*

Summary

On Tuesday, September 21, 2021, VMware has released VMSA-2021-0020 advisory [1] to address multiple vulnerabilities in vCenter Server and Cloud Foundation appliances that a remote attacker could exploit to take control of an affected system. The most urgent and critical is a file upload vulnerability **CVE-2021-22005** that can be used to execute commands and software on the vCenter Server Appliance [2].

On Tuesday, September 24, 2021 VMware updated the advisory VMSA-2021-0020.1 and confirmed reports that **CVE-2021-22005 is being exploited** in the wild [1]. Security researchers are also reporting **mass scanning** for vulnerable vCenter Servers and publicly available exploit code [5, 6, 7].

Technical Details

A malicious actor with network access to port 443 on vCenter Server may exploit **CVE-2021-22005 (CVSSv3 base score of 9.8)** vulnerability to execute code on vCenter Server by uploading a specially crafted file, **regardless of the configuration settings of vCenter Server** [1, 2].

Affected Products

The **CVE-2021-22005** vulnerability impacts following versions [4]:

- VMware vCenter Server 6.7
- VMware vCenter Server 7.0

This issue (CVE-2021-22005) does not affect vCenter Server 6.5 [1].

Recommendations

VMware recommends affected customers to install relevant updates as soon as possible.

Workarounds

VMware also provides a workaround for those who cannot immediately patch their appliances as a temporary solution [3].

References

[1] https://www.vmware.com/security/advisories/VMSA-2021-0020.html

[2] https://blogs.vmware.com/vsphere/2021/09/vmsa-2021-0020-what-you-need-to-know.html

[3] https://kb.vmware.com/s/article/85717

[4] https://www.bleepingcomputer.com/news/security/vmware-warns-of-critical-bug-in-default-vcenter-server-installs/

[5] https://us-cert.cisa.gov/ncas/current-activity/2021/09/24/vmware-vcenter-server-vulnerability-cve-2021-22005-under-active

[6] https://twitter.com/bad_packets/status/1441465508348317702

[7] https://www.bleepingcomputer.com/news/security/hackers-exploiting-critical-vmware-vcenter-cve-2021-22005-bug/