Hive Pro

THREAT ADVISORY

VMWare VCenter affected by multiple RCE Vulnerabilities

TA202112

Threat Level Red

Publish Date – May 26, 2021

Multiple Remote code execution vulnerabilities have been patched by VMWare today. These vulnerabilities (CVE-2021-21985, CVE-2021-21986) exists due to lack of validation in vSAN(Virtual SAN) Health Check Plug-in which is a default plug-in in vCenter Server. Anyone with an unauthorized network access to port 443 can exploit these by executing commands which do not require any privileges on the OS where vCenter server exists.

Vulnerability Details

CVE ID	Affected Versions	Affected CPEs	Vulnerability Name
CVE-2021-21985	vCenter Server versions 7.0,6.7,6.5 Cloud Foundation (vCenter Server) versions 4.x,3.x	cpe:2.3:a:vmware:vcenter_server:6.5:-:*:*:*:*:*:* cpe:2.3:a:vmware:vcenter_server:6.7:*:*:*:*:*:*:* cpe:2.3:a:vmware:vcenter_server:7.0:*:*:*:*:*:*:* cpe:2.3:a:vmware:cloud_foundation:3.0:*:*:*:*:*:*:* cpe:2.3:a:vmware:cloud_foundation:4.0:*:*:*:*:*:*:*	VMware vCenter Server updates address remote code execution vulnerability in the vSphere Client
CVE-2021-21986			Authentication mechanism issue in vCenter Server Plug-ins

Patch Links

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

References

https://thehackernews.com/2021/05/critical-rce-vulnerability-found-in.html
https://www.tenable.com/blog/cve-2021-21985-critical-vmware-vcenter-server-remote-code-execution?utm_source=feedburner&utm_medium=feed&utm_campaign=Feed%3A+tenable%2FqaXL+%28Tenable+Network+Security+Blog%29