Hive Pro

THREAT ADVISORY

VMware patches SSRF and arbitrary file read vulnerabilities in vCenter Server

TA202151

Threat Level AMBER

Publish Date – Nov 25, 2021

VMware has released fixes to address two security flaws in vCenter Server and Cloud Foundation ,tracked as CVE-2021-21980 and CVE-2021-22049. The vulnerability CVE-2021-21980 (arbitrary file read) is of major concern as an attacker with network access to port 443 on vCenter Server can use this vulnerability to gain access to sensitive data.

Another vulnerability CVE-2021-22049 is an SSRF(Server-Side Request Forgery) vulnerability in the VSAN Web Client plug-in which a hostile actor with network access to port 443 on vCenter Server to exploit the flaw by visiting an internal service or a URL request outside of the server.

VMware has not released any official workarounds for the vulnerabilities, but organizations can patch their vulnerabilities for vCenter Server from the patch link provided down below. Patches for both the vulnerabilities are still pending for Cloud Foundation version 3.x.

Vulnerability Details

CVE ID	Affected Products	Affected CPE	Vulnerability Name	CWE ID
CVE-2021-21980	VMware vCenter Server prior to version 6.7 and Cloud Foundation prior to version 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:cloud_foundation:3.0:*:*:*:*:*:*:*	VMware vCenter Server information disclosure	CWE-200
CVE-2021-22049			VMware vCenter Server server-side request forgery	CWE-918

Patch Link

https://www.vmware.com/security/advisories/VMSA-2021-0027.html

References

https://portswigger.net/daily-swig/vmware-addresses-ssrf-arbitrary-file-read-flaws-in-vcenter-server
https://thehackernews.com/2021/11/vmware-warns-of-newly-discovered.html