Security Advisory 2021-065

Vulnerabilities in VMware Products

November 25, 2021 — v1.0

TLP:WHITE

History:

- *22/09/2021 — v1.0 – Initial publication*

Summary

On November 23, VMWare has released the VMSA-2021-0027 advisory [1] that addresses two vulnerabilities in vCenter Server and Cloud Foundation. An attacker could exploit these vulnerabilities to read sensitive files (`CVE-2021-21980` - unauthorised arbitrary file read vulnerability) or to induce the server to make connections to arbitrary destinations (`CVE-2021-22049` - SSRF vulnerability).

Technical Details

The vulnerability `CVE-2021-21980` (CVSSv3 score of 7.5 out of 10) could allow a remote attacker with network access to port 443 on vCenter Server to gain access to sensitive information by reading unauthorised files on the server.

The vulnerability `CVE-2021-22049` (CVSSv3 score of 6.5 out of 10) could allow a remote attacker with network access to port 443 on vCenter Server to read or modify internal resources that the target server has access to, by sending specially crafted HTTP requests, resulting in the unauthorised exposure of information [2].

Affected Products

The `CVE-2021-21980` and `CVE-2021-22049` vulnerabilities impact the following versions [1]:

- VMWare vCenter Server versions 6.5 and 6.7
- VMware Cloud Foundation version 3.x (the patch is pending)

Recommendations

VMware and CERT-EU recommend installing relevant updates when possible and monitoring the release of the patch for the VMware Cloud Foundation product.

References

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

[2] https://portswigger.net/web-security/ssrf