UNISPHERE SOLUTIONS

info@unisphere.co.nz
www.unisphere.co.nz

CYBER GUIDANCE ISSUE 00202

VULNERABILITIES IN VMWARE VCENTER SERVER

DATE ISSUED: 27th September 2021

IMPACT	LOW	MEDIUM	[✓ HIGH]
EASE OF EXPLOIT	HARD	MEDIUM	[✓ EASY]

OVERVIEW

VMWare have released updates for 19 CVEs – including one rated CRITICAL - for the vCenter Server virtualisation management platform and Cloud Foundation platform as attackers are known to be actively scanning for vulnerable servers to exploit.

BREAKDOWN

The most critical of the CVEs rated 9.8 is CVE-2021-22005 which could allow a files to be uploaded to the Virtual Machine (VM) if a server is able to be reached over the Internet. Affected versions of vCenter include 6.5, 6.7 and 7.0. By uploading a file, attackers could easily upload anything they like, including malicious software such as ransomware within minutes of discovering the flaw. While the other flaws are not rated as highly, they are still considered relatively easy to exploit or use to move laterally across a network once a system is compromised.

REMEDIATION STEPS

- Apply latest security patches and updates immediately – this patch is considered an emergency change. If this is not possible, use the workaround provided in the resources listed below.
- Assume your systems have been compromised and look for indicators of such.
- It is important to have a firm grasp on the assets you own and conduct asset and patch management activities regularly. You can’t patch something if you don’t know it’s there.
- Make sure your network perimeter controls (such as firewall firmware) are patched and have the appropriate controls (policies and rules) configured.
- Limit access to vCenter Server, ESXi and vSphere management interfaces with strong admin passwords in place

REFERENCES & RESOURCES

VMWare	https://core.vmware.com/vmsa-2021-0020-questions-answers-faq https://www.vmware.com/security/advisories/VMSA-2021-0020.html
Threatpost	https://threatpost.com/vmware-ransomware-bug-vcenter-server/174901/
CERT NZ	https://www.cert.govt.nz/it-specialists/advisories/active-scanning-for-vmware-vcenter-vulnerability/
ZDNet	https://www.zdnet.com/article/rce-is-back-vmware-details-file-upload-vulnerability-in-vcenter-server