UNISPHERE SOLUTIONS
info@unisphere.co.nz
www.unisphere.co.nz

CYBER GUIDANCE ISSUE 00112

VMWARE PATCHES CRITICAL RCE FLAW

DATE ISSUED: 2nd March 2021

IMPACT	LOW	MEDIUM	**HIGH**
EASE OF EXPLOIT	HARD	MEDIUM	**EASY**

OVERVIEW

Three vulnerabilities have been taken care of this week by VMWare in the vCenter Server Management Platform that could have allowed attackers to breach a data centre perimeter or use previously planted backdoors to perform a system take over. CVE-2021-21972

BREAKDOWN

Rating 9.8/10 on the CVSS scale, this exploit takes advantage of the vCenter Server plugin for vROPs in the vSphere Client through port 443 through which an attacker may be able to execute commands with full access privileges. This plugin is installed by default in many installations and is most vulnerable to insider threats or those who have already gained access through the network perimeter and can be exploited by any unauthorised user. External attackers can leverage the loophole in instances where access is available via the internet.

Further flaws patched by VMWare this week include CVE-2021-21974 affecting the hypervisor VMWare ESXi and CVE-2021-21973 which can lead to Server Side Request Forgery due to the vCenter Server plugin improperly validating URLs.

REMEDIATION STEPS

- Apply all security patches issued by VMWare – workarounds are available for those who are unable to apply these patches immediately.
- Check VMWare virtual machine configuration and security to ensure only necessary services can be accessed through the internet and proper authentication mechanisms are enabled.
- Conduct penetration testing to assess your cloud/virtual environment and create a remediation action plan.

REFERENCES & RESOURCES

Threatpost https://threatpost.com/vmware-patches-critical-rce-flaw-in-vcenter-server/164240/
VMWare https://www.vmware.com/security/advisories/VMSA-2021-0002.html