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

CYBER GUIDANCE ISSUE 00149

VMWARE CRITICAL VCENTER RCE FLAW

DATE ISSUED: 31st May 2021

IMPACT	LOW	MEDIUM	HIGH
EASE OF EXPLOIT	HARD	MEDIUM	EASY

OVERVIEW

Two notable vulnerabilities and CVE-2021-21985 (scoring 9.8/10) relates to Remote Code Execution (RCE) over port 443 in the vSAN plugin – a default plugin in vCenter, and CVE-2021-21986 (scoring 6.5/10) enables attackers to perform actions allowed by plugins without authentication.

BREAKDOWN

As vSAN is enabled by default, users who do not directly use the Virtual SAN Health Check plugin may find they are affected by this vulnerability that occurs in the vSphere Client (HTML5) due to a lack of input validation. vCenter Servers that have direct access to the Internet are incredibly vulnerable as all an attacker needs to do it hit port 443 to gain access. These servers should be audited and update immediately. Firewall controls are the only line of defence in other cases, and may not be relevant if an attacker is already within the perimeter of your network – as is the case with many ransomware attacks.

REMEDIATION STEPS

- Update vCenter Servers versions 6.5, 6.7 and 7.0 immediately. The patches provide better plugin authentication which may cause issues with other third-party plugins and users are advices to contact the plugin vendor should this occur.
- Use a Reverse Proxy and a firewall between any web servers and the Internet as added layers of protection against direct access to web-facing servers and/or isolate web servers from the main network using a DeMilitarised Zone (DMZ) and firewalls.
- Disable the vCenter plugin using the instructions provided by VMWare https://kb.vmware.com/s/article/83829

REFERENCES & RESOURCES

VMWare https://www.vmware.com/security/advisories/VMSA-2021-0010.html
ZDNet https://www.zdnet.com/article/patch-immediately-vmware-warns-of-critical-remote-code-execution-holes-in-vcenter
ARS Technica https://arstechnica.com/gadgets/2021/05/vulnerability-in-vmware-product-has-severity-rating-of-9-8-out-of-10/