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

CYBER GUIDANCE ISSUE 00114

URGENT SECURITY UPDATE: MICROSOFT EXCHANGE

DATE ISSUED: 3rd March 2021

IMPACT	LOW	MEDIUM	HIGH
EASE OF EXPLOIT	HARD	MEDIUM	EASY

OVERVIEW

Multiple vulnerabilities are being exploited by attackers enabling them to gain access to Microsoft Exchange Servers – especially those with exposure to the internet, with full system privileges which may lead to potential network compromise and the exfiltration of sensitive data.

BREAKDOWN

Although Microsoft Exchange Online is not affected by this threat, on-premise Microsoft Exchange Servers are under known attack by a sophisticated threat actor, as multiple zero-day attacks are under investigation by the Microsoft Threat Intelligence Centre (MSTIC). The attacker is suspected to be the HAFNIUM group. The attacks thus far have seen access to email accounts and the ability for the attacker to deploy further malware to facilitate long-term access to systems and environments – in other words, installing a backdoor or an Advanced Persistent Threat (APT). The vulnerabilities are considered critical and should be remediated immediately.

CVE-2021-26855, CVE-2021-26857, CVE-2021-26858, and CVE-2021-27065.

REMEDIATION STEPS

- Install patches and security updates released today for Microsoft Exchange Server versions 2013, 2016, 2019 – although 2010 is considered out of support, there is still a patch available for this version.
- See Microsoft resources below for a full list of Indicators of Compromise (IoCs) and further CVE info.
- Report any incidents of breach to CERT NZ by calling 0800 CERTNZ or via their website https://www.cert.govt.nz/it-specialists/report-an-incident/

REFERENCES & RESOURCES

CERT NZ	https://www.cert.govt.nz/it-specialists/advisories/urgent-microsoft-exchange-security-update/
Microsoft Security Blog	https://www.microsoft.com/security/blog/2021/03/02/hafnium-targeting-exchange-servers/
Security Response Center	https://msrc-blog.microsoft.com/2021/03/02/multiple-security-updates-released-for-exchange-server/