U UNISPHERE SOLUTIONS

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

CYBER GUIDANCE ISSUE 00039

'ZEROLOGON' EXPLOIT IN WINDOWS

DATE ISSUED: 21st September 2020

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

OVERVIEW

"Zerologon" is named so because it is presented as a flaw in Microsoft's Active Directory and domain controllers that could allow an attacker to gain access to a network simply by plugging in to an on-premise port – no login required. CVE-2020-1472

BREAKDOWN

Released in the bundle of Microsoft's security patches for August 2020, this exploit has been investigated by a number of independent testers using the Proof of Concept (PoC) method and discovered numerous means to compromise a Windows domain. Although the attacker would need access to the same LAN as their intended target, they would be able to gain full access whilst completely unauthenticated – that is, not requiring a set of login credentials. The origin of the flaw in the Netlogon Remote Protocol which is used in authenticating connected machines where the Initialisation Vector (IV) is set to a fixed 16bits that may be deciphered by an attacker to impersonate any machine on the network.

REMEDIATION STEPS

- Ensure all devices connected to the LAN have the latest Microsoft security patched installed
- Monitor network for unusual activity – particularly any new connections or new ports in use.
- Ensure technical and management controls are in place to ensure all domain controllers are updated before connecting to the network.
- Stay alert to further patch releases

REFERENCES & RESOURCES

Threatpost:	https://threatpost.com/windows-exploit-microsoft-zerologon-flaw/159254/
Cyber.dhs.gov:	https://cyber.dhs.gov/ed/20-04/
Tenable:	https://www.tenable.com/cve/CVE-2020-1472
IT News AU	https://www.itnews.com.au/news/zerologon-windows-domain-admin-bypass-exploit-released-553317
ZDNet:	https://www.zdnet.com/article/zerologon-attack-lets-hackers-take-over-enterprise-networks/