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

CYBER GUIDANCE ISSUE 00088

WINDOWS ZERO-DAY REMAINS UNFIXED

DATE ISSUED: 12th January 2021

IMPACT	LOW	MEDIUM	HIGH
EASE OF EXPLOIT	HARD	MEDIUM	EASY

OVERVIEW

A fix issued by Microsoft to combat a dangerous Local Privilege Escalation (LPE) flaw has failed to adequately patch the vulnerability that could allow full takeover of a system. CVE-0020-0986

BREAKDOWN

Existing in the Print Spooler API of Windows 8.1 and 10 operating systems, this vulnerability could allow an attacker to create new accounts or elevate privileges on compromised existing accounts, allowing full control of the system. After logging in to a system, an attacker would run a bespoke application to exploit the kernel's inability to properly handle objects in memory using arbitrary code. This type of attack may be used to generate a buffer overflow or deploy an Advanced Persistent Threat (APT). There are known instances of this attack occurring in the wild and the first patch was released June 2020. The newly issued CVE-2020-17008 rates at 8.3/10 on the CVSS scale and a further patch is expected in the January update.

REMEDIATION STEPS

- Monitor systems for unusual log in activity and scan systems using anti-malware software to detect abnormal behaviour
- Restrict user's ability to run .exe files on their machines where there is no need to have this capability
- Apply January patches from Microsoft expected to be released 13/01/2021

REFERENCES & RESOURCES

Threatpost: https://threatpost.com/windows-zero-day-circulating-faulty-fix/162610/
Cybersecurity-help https://www.cybersecurity-help.cz/vdb/SB2020122401