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

CYBER GUIDANCE ISSUE 00164

PRINT SPOOLER PRINTNIGHTMARE & MANY MORE

DATE ISSUED: 5th July 2021

IMPACT	LOW	MEDIUM	HIGH
EASE OF EXPLOIT	HARD	MEDIUM	EASY

OVERVIEW

Numerous vulnerabilities across a range of Microsoft products have been uncovered with six of these zero-days under active exploitation in the wild and researchers have proven that the patched which are currently available may not be enough to prevent exploitation.

BREAKDOWN

An attacker may be able to gain system level access on any affected Windows device where the Print Spooler service is enabled allowing them to install programs, read, alter, or delete data, create new users accounts with full access and much more. Print Spooler is enabled by default on Windows Domain Controller and affects those that have Point and Print configured with the NoWarningNoElevationOnInstall option. CVE-2021-1675 has been partially addressed in the Patch Tuesday June 2021 release but there are still some flaws that may be exploited, coupled with the release of information regarding a further vulnerability CVE-2021-34527 allowing Remote Code Execution (RCE). A Proof of Concept (PoC) was published on GitHub and although the original post has been removed, the code continues to circulate on the platform after being copied by users. The six zero-days noted as being under active attack are CVE-2021-1675, CVE-2021-33742, CVE-2021-33739, CVE-52021-31199, CVE-31201-39155 and CVE-2021-31956.

REMEDIATION STEPS

- Apply patches (Issued June 2021) or appropriate workaround provided by Microsoft (CVE-2021-34527).
- Disable the Print Spooler service on any machines that don't require it.
- Software should not be run as an administrator - all software should be run as a non-privileged user.
- Educate users on the dangers of phishing attacks, social engineering and visiting unknown/untrusted or malicious sites and what the process is in your organisation for reporting suspicious emails.
- Monitor communications from Microsoft as the situation continues to evolve.

REFERENCES & RESOURCES

CERT NZ	https://www.cert.govt.nz/it-specialists/advisories/critical-vulnerability-in-microsoft-windows-print-spooler-service
ZDNet	https://www.zdnet.com/article/microsoft-adds-second-cve-for-printnightmare-remote-code-execution
Threatpost	https://threatpost.com/poc-exploit-windows-print-spooler-bug/167430/ + https://threatpost.com/cisa-mitigation-printnightmare-bug/167515/
Microsoft	https://msrc.microsoft.com/update-guide + https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-34527
MS-ISAC	Center for Internet Security Advisory