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

CYBER GUIDANCE ISSUE 00170

FURTHER PRINT SPOOLER VULNERABILITIES

DATE ISSUED: 19th July 2021

IMPACT	LOW	MEDIUM	**HIGH**
EASE OF EXPLOIT	HARD	**MEDIUM**	EASY

OVERVIEW

Hot on the heels of the PrintNightmare Print Spooler vulnerabilities set, a further vulnerability has been discovered by Dragos that allows privilege escalation to be performed by attackers.

BREAKDOWN

CVE-2021-34481 exists within the Window Print Spooler service and is prone to improperly performing privileged file operations as once exploited, attackers are able to run arbitrary code with full System level privileges. This may lead to installation or removal of programs, read access, modification or destruction of data or creating further user accounts with full access privileges. Additional vulnerabilities unrelated to the PrintNightmare attacks have surfaced including CVE-2021-1675 rated 7.8/10 on the CVSS scale which can only be exploited with local access.

REMEDIATION STEPS

- Official advice from Microsoft is to disable the Print Spooler services.
- Install all other Windows security and emergency patches available – these fixes are not complete and do not include the vulnerability that is the focus of this email.

REFERENCES & RESOURCES

Threatpost https://threatpost.com/microsoft-unpatched-bug-windows-print-spooler/167855/
Microsoft https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-34481