UNISPHERE SOLUTIONS

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

CYBER GUIDANCE ISSUE 00175

PRINTER VULNERABILITY IN HP, XEROX & SAMSUNG

DATE ISSUED: 26th July 2021

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

OVERVIEW

A vulnerability in the SSPORT.SYS Print Driver affecting hundreds of millions of devices allows local privilege escalation giving attackers system access and the ability to run code in kernel mode, bypassing security controls.

BREAKDOWN

Printers and other peripheral devices connected to our networks often get forgotten when it comes to patching. HP, Xerox and Samsung printers are affected by a vulnerability that has been present since 2005 and could allow an attacker to gain entry to a system and elevate their own privileges or create new accounts with full access by running arbitrary code in kernel mode. This flawed driver is automatically installed with printer software and is loaded by Windows after each restart, making it a juicy target. This would also give the attacker the ability to bypass security products, install programs – including malware, as well as read, write, alter, delete, or encrypt data. At this stage there are no reports of this vulnerability being exploited in the wild and requires local privileges to be executed. CVE-2021-3438

REMEDIATION STEPS

- Apply the latest patches to your printer from the vendor.
- Users should only be able to run software as a general user, not an administrator which will reduce the effects of a successful attack.
- Use the principle of Least Privilege when granting user access rights.

REFERENCES & RESOURCES

Bleeping Computer	https://www.bleepingcomputer.com/news/security/16-year-old-bug-in-printer-software-gives-hackers-admin-rights/
HP	https://support.hp.com/us-en/document/ish_3900395-3833905-16/hpsbpi03724
Xerox	https://securitydocs.business.xerox.com/wp-content/uploads/2021/05/cert_Security_Mini_Bulletin_XRX21K_for_B2XX_PH30xx_3260_3320_WC3025_32xx_33xx.pdf
CIS Advisory Newsletter	