The following security alert was issued by the Information Security Division of the Mississippi Department of ITS and is intended for State government entities. The information may or may not be applicable to the general public and accordingly, the State does not warrant its use for any specific purposes.

TLP: WHITE
https://www.cisa.gov/tlp
Sources may use TLP:WHITE when information carries minimal or no foreseeable risk of misuse, in accordance with applicable rules and procedures for public release. Subject to standard copyright rules, TLP:WHITE information may be distributed without restriction.

DATE(S) ISSUED:
07/20/2021

SUBJECT:
A Vulnerability in HP, Xerox, and Samsung Printer Drivers Could Allow Attackers to Gain Administrator Rights on a System

OVERVIEW:
A vulnerability has been discovered HP, Xerox, and Samsung printer drivers, which could result in local privilege escalation. A printer driver is a piece of system software that allows your computer to interact with your printer. This vulnerability specifically deals with an old printer driver from 2005 called SSPORT.SYS which affects hundreds of millions of devices and millions of users worldwide. Successfully exploitation of this vulnerability might allow attackers to potentially install programs, view, change, encrypt or delete data, or create new accounts with full user rights.

THREAT INTELLIGENCE:
There are no reports of this vulnerability being exploited in the wild

SYSTEMS AFFECTED:

- Please refer to the reference section for the full list of systems affected for HP and Xerox

RISK:
Government:

- Large and medium government entities: **High**
- Small government entities: **Medium**

Businesses:

- Large and medium business entities: **High**
- Small business entities: **Medium**

Home users: Low

TECHNICAL SUMMARY:
A vulnerability has been discovered in HP, Xerox, and Samsung printer drivers which could result in local privilege escalation. HP, Xerox, and Samsung are prone to a local privilege escalation vulnerability that could allow a user with basic user privileges to elevate their privileges to SYSTEM and run code in kernel mode, potentially bypassing security products that would block their attacks or the delivery of additional malicious payloads. Successfully exploiting

this vulnerability (SSPORT.SYS) might allow attackers to potentially install programs, view, change, encrypt or delete data, or create new accounts with full user rights.

RECOMMENDATIONS:
The following actions should be taken:

- Apply the latest patches provided by HP and Xerox
- Run all software as a non-privileged user (one without administrative privileges) to diminish the effects of a successful attack.
- Remind users not to visit un-trusted websites or follow links provided by unknown or un-trusted sources.
- Inform and educate users regarding the threats posed by hypertext links contained in emails or attachments especially from un-trusted sources.
- Apply the Principle of Least Privilege to all systems and services.

REFERENCES:
Bleeping Computer:
https://www.bleepingcomputer.com/news/security/16-year-old-bug-in-printer-software-gives-hackers-admin-rights/

CVE:
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-3438

HP (Affected Systems/Patch):
https://support.hp.com/us-en/document/ish_3900395-3833905-16/hpsbpi03724

SentinelOne:
https://labs.sentinelone.com/cve-2021-3438-16-years-in-hiding-millions-of-printers-worldwide-vulnerable/

XP (Affected Systems/Patch):
https://securitydocs.business.xerox.com/wp-content/uploads/2021/05/cert_Security_Mini_Bulletin_XRX21K_for_B2XX_PH30xx_3260_3320_WC3025_32xx_33xx.pdf

TLP: WHITE
https://www.cisa.gov/tlp
Sources may use TLP:WHITE when information carries minimal or no foreseeable risk of misuse, in accordance with applicable rules and procedures for public release. Subject to standard copyright rules, TLP:WHITE information may be distributed without restriction.