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:
12/01/2021

SUBJECT:
A Vulnerability in HP Printer Products Could Allow for Arbitrary Code Execution.

OVERVIEW:
A vulnerability has been discovered in HP FutureSmart that could allow for arbitrary code execution. HP FutureSmart is a piece of system firmware that is used on all HP Enterprise devices. Successful exploitation of this vulnerability could allow for arbitrary code execution within the context of the affected application. Depending on the privileges associated with this application, an attacker could then install programs; view, change, or delete data; or create new accounts with full user rights. If this application has been configured to have fewer user rights on the system, exploitation of this vulnerability could have less impact than if it was configured with administrative rights.

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

SYSTEMS AFFECTED:
- HP Futuresmart 3 cpe:/h:hp:futuresmart_3 DS
- HP Futuresmart 4 cpe:/h:hp:futuresmart_4 DS
- HP Futuresmart 5 cpe:/h:hp:futuresmart_5 DS

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 FutureSmart that could allow for arbitrary code execution. Vulnerable HP FutureSmart versions are susceptible to a buffer overflow vulnerability that may result in the ability for a remote and unauthenticated attacker to execute arbitrary code on the targeted systems.

Successful exploitation of this vulnerability could allow for arbitrary code execution within the context of the affected application. Depending on the privileges associated with this application, an attacker could then install programs; view, change, or delete data; or create new accounts with full user rights. If this application has been configured to have fewer user rights on the system, exploitation of this vulnerability could have less impact than if it was configured with administrative rights.

RECOMMENDATIONS:
The following actions should be taken:

- Apply the latest patches provided by HP after appropriate testing.
- 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:
CVE:
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-39238

HP:
https://support.hp.com/us-en/document/ish_5000383-5000409-16
https://www.hp.com/us-en/printers/futuresmart-firmware.html

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.