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:
02/01/2022

SUBJECT:
A Vulnerability in Samba Could Allow for Arbitrary Code Execution

OVERVIEW:
A vulnerability has been discovered in Samba which could allow for arbitrary code execution. Samba is the standard Windows interoperability suite of programs for Linux and Unix. Successful exploitation of this vulnerability could result in arbitrary code execution as root on affected Samba installations that use the VFS module vfs_fruit. Depending on the permission associated with the application running the exploit, an attacker could then install programs; view, change, or delete data.

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

SYSTEMS AFFECTED:

- Samba prior to version 4.13.17

RISK:
Government:

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

Businesses:

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

Home users: Low

TECHNICAL SUMMARY:
A vulnerability has been discovered in Samba installations that use the vfs_fruit module, which could allow for arbitrary code execution. An out-of-bounds heap read write vulnerability exists within the parsing of EA metadata when opening files in smbd. Access as a user that has write access to a file's extended attributes is required to exploit this vulnerability. This could be a guest or unauthenticated user if such users are allowed write access to file extended attributes. The problem in vfs_fruit exists in the default configuration of the fruit VFS module using fruit:metadata=netatalk or fruit:resource=file. If both options are set to different settings than the default values, the system is not affected by the security issue.

Successful exploitation of this vulnerability could result in arbitrary code execution as root on affected Samba installations. Depending on the permission associated with the application running the exploit, an attacker could then install programs; view, change, or delete data.

RECOMMENDATIONS:

The following actions should be taken:

- Apply appropriate patches provided by Samba to vulnerable systems and servers immediately after appropriate testing.
- Run all software as a non-privileged user (one without administrative privileges) to diminish the effects of a successful attack.
- Evaluate read, write, and execute permissions on all newly installed software.
- Apply the Principle of Least Privilege to all systems and services.

REFERENCES:

Samba:

https://www.samba.org/samba/security/CVE-2021-44142.html

CVE:

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-44142

The Hacker News:

https://thehackernews.com/2022/01/new-samba-bug-allows-remote-attackers.html