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
www.cisa.gov/tlp
Information may be distributed without restriction, subject to standard copyright rules.

DATE(S) ISSUED:
07/29/2022

SUBJECT:
Multiple Vulnerabilities in Samba Could Allow for Privilege Escalation

OVERVIEW:
Multiple vulnerabilities have been discovered in Samba, the most severe of which could allow for privilege escalation. Samba is the standard Windows interoperability suite of programs for Linux and Unix. Successful exploitation of the most severe of these vulnerabilities, could allow any user to escalate privileges to administrator, and gain total control over the domain.

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

SYSTEMS AFFECTED:

- Samba versions prior to 4.16.4, 4.15.9, and 4.14.14

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:
Multiple Vulnerabilities have been discovered in Samba, the most severe of which could allow for Privilege Escalation. Details of these vulnerabilities are as follows:

Tactic: *Privilege Escalation* (TA0029):

Technique: *Exploitation for Privilege Escalation* (T1404):

- CVE-2022-32744 – A vulnerability in the Password Change Handler component could allow a local user to change the passwords of other users, enabling full domain takeover.
- CVE-2022-2031 – A vulnerability in the KDC/password service could allow a local user escalate privileges.

Details of lower-severity vulnerabilities are as follows:

- CVE-2022-32745 – A vulnerability in the LDAP Handler could allow a local user to cause a segmentation fault. This could allow a local user to crash the server process.
- CVE-2022-32746 – A vulnerability in Sambas AD DC Database Audit Logging could result in a use-after-free. This could allow a local user to cause a corrupted output or crash.
- CVE-2022-32742 – A vulnerability in the Samba SMB1 component could allow for memory corruption. This could allow server memory contents to be written into a file.

Successful exploitation of the most severe of these vulnerabilities, could allow any user to escalate privileges to administrator, and gain total control over the domain.

RECOMMENDATIONS:

We recommend the following actions be taken:

- Apply appropriate patches provided by Samba to vulnerable systems, immediately after appropriate testing. (**M1051: Update Software**)
    - **Safeguard 7.1: Establish and Maintain a Vulnerability Management Process**: Establish and maintain a documented vulnerability management process for enterprise assets. Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.
    - **Safeguard 7.4: Perform Automated Application Patch Management:** Perform application updates on enterprise assets through automated patch management on a monthly, or more frequent, basis.
    - **Safeguard 7.5: Perform Automated Vulnerability Scans of Internal Enterprise Assets:** Perform automated vulnerability scans of internal enterprise assets on a quarterly, or more frequent, basis. Conduct both authenticated and unauthenticated scans, using a SCAP-compliant vulnerability scanning tool.
- Remind users not to visit un-trusted websites or follow links provided by unknown or un-trusted sources. Inform and educate users regarding threats posed by hypertext links contained in emails or attachments, especially from un-trusted sources. (**M1017: User Training**)

    - **Safeguard 14.1: Establish and Maintain a Security Awareness Program:** Establish and maintain a security awareness program. The purpose of a security awareness program is to educate the enterprise's workforce on how to interact with enterprise assets and data in a secure manner. Conduct training at hire and, at a minimum, annually. Review and update content annually, or when significant enterprise changes occur that could impact this Safeguard.
    - **Safeguard 14.2: Train Workforce Members to Recognize Social Engineering Attacks:** Train workforce members to recognize social engineering attacks, such as phishing, pre-texting, and tailgating.
- Use capabilities to detect and block conditions that may lead to or be indicative of a software exploit occurring. (**M1050: Exploit Protection)**

Safeguard 10.5: Enable anti-exploitation features on enterprise assets and software, where possible, such as Apple® System Integrity Protection (SIP) and Gatekeeper™.

REFERENCES:

Samba:https://www.samba.org/samba/history/security.html
https://www.samba.org/samba/security/CVE-2022-2031.html
https://www.samba.org/samba/security/CVE-2022-32742.html
https://www.samba.org/samba/security/CVE-2022-32744.html
https://www.samba.org/samba/security/CVE-2022-32745.html
https://www.samba.org/samba/security/CVE-2022-32746.html

CVE:https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-2031
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-32742
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-32744
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-32745
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-32746