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:
03/08/2022

SUBJECT:
A Vulnerability in Linux Kernel Could Allow for Data Overwrite in Arbitrary Read-Only Files - PATCH: NOW - TLP: WHITE

OVERVIEW:
A vulnerability has been discovered in the Linux kernel, which could allow for data overwrite in arbitrary read-only files by non-privilege users. Linux is a family of open-source Unix-like operating systems based on the Linux kernel. Successful exploitation of this vulnerability could allow for root privilege escalation.

THREAT INTELLIGENCE:
There is currently a publicly available proof of concept for the exploitation of this vulnerability.

SYSTEMS AFFECTED:
- Linux Kernels version 5.8 to 5.16.10, 5.15.24 and 5.10.101

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: Medium

TECHNICAL SUMMARY:

A vulnerability has been discovered in the Linux kernel, which could allow for data overwrite in arbitrary read-only files by non-privilege users. Linux is a family of open-source Unix-like operating systems based on the Linux kernel. Successful exploitation of this vulnerability could allow for root privilege escalation through the editing of administrative files such as /etc/passwd.

RECOMMENDATIONS:

The following actions should be taken:

- Update affected systems to kernel versions that have remediated the vulnerability.
- Remind users not to visit un-trusted websites or follow links provided by unknown or un-trusted sources.
- Apply the Principle of Least Privilege to all systems and services.

REFERENCES:

Git:

https://learn.cisecurity.org/e/799323/4e13b2a0546fee6737ee4446017903/rrgfz/269390719?h=wqEFKRUfm-LwdlqZmoW40Kwmzz17hCccvIfkIy6beXQ

Max Kellerman:

https://dirtypipe.cm4all.com/

CVE:

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-0847