*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**
**Disclosure is not limited. Subject to standard copyright rules, TLP: WHITE information may be distributed without restriction.**
**http://www.us-cert.gov/tlp/**

**DATE(S) ISSUED:**
02/17/2021

**SUBJECT:**
A Vulnerability in WebKitGTK and WPE WebKit Could Allow for Arbitrary Code Execution

**OVERVIEW:**
A vulnerability has been discovered in WebKit GTK and WPE WebKit which could allow for arbitrary code execution.

- WebKitGTK is a full-featured port of the WebKit rendering engine, suitable for projects requiring any kind of web integration, from hybrid HTML/CSS applications to full-fledged web browsers.
- WPE is the reference WebKit port for embedded and low-consumption computer devices.

Successful exploitation of this vulnerability could allow for arbitrary code execution. Depending on the privileges associated with the user an attacker could then install programs; view, change, or delete data; or create new accounts with full user rights. Users whose accounts are configured to have fewer user rights on the system could be less impacted than those who operate with administrative user rights.

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

**SYSTEMS AFFECTED:**
- WebKitGTK prior to version 2.30.5
- WPE WebKit prior to version 2.30.5

**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 WebKitGTK and WPE WebKit which could allow for arbitrary code execution. This vulnerability occurs when processing specially crafted web content due to a use after free error in the 'AudioSourceProviderGStreamer' class.

Successful exploitation of this vulnerability could allow an attacker to execute arbitrary code in the context of the browser. 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:

- Install the updates provided by WebKitGTK and WPE WebKit immediately 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:**
**WebKitGTK:**
https://webkitgtk.org/security/WSA-2021-0001.html

**WPE WebKit:**
https://wpewebkit.org/security/WSA-2021-0001.html

**CVE:**
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-13558