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

DATE(S) ISSUED:
02/11/2022

SUBJECT:
A Vulnerability in Apple Products Could Allow for Arbitrary Code Execution

OVERVIEW:
A vulnerability has been discovered in Apple Products, which could allow for arbitrary code execution if a user views a specially crafted web page.

- iOS is a mobile operating system for mobile devices, including the iPhone, iPad, and iPod touch.
- iPadOS is the successor to iOS 12 and is a mobile operating system for iPads.
- macOS Monterey is the 18th and current major release of macOS.
- Safari is a graphical web browser developed by Apple.

Successful exploitation of this vulnerability could result in arbitrary code execution within the context of the application, an attacker gaining the same privileges as the logged-on user, or the bypassing of security restrictions. Depending on the permission associated with the application running the exploit, an attacker could then install programs; view, change, or delete data.

THREAT INTELLIGENCE:
Apple is aware of a report that CVE-2022-22620 may have been actively exploited.

SYSTEMS AFFECTED:

- iOS and iPadOS prior to 15.3.1
- macOS Monterey prior to 12.2.1
- Safari prior to 15.3 (v. 16612.4.9.1.8 and 15612.4.9.1.8)

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 Apple Products, which could allow for arbitrary code execution if a user views a specially crafted web page.

Successful exploitation of this vulnerability could result in arbitrary code execution within the context of the application, an attacker gaining the same privileges as the logged-on user, or the bypassing of security restrictions. Depending on the permission associated with the application running the exploit, an attacker could then install programs; view, change, or delete data.

RECOMMENDATIONS:
We recommend the following actions be taken:

- Apply appropriate patches provided by Apple to vulnerable systems 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 download, accept or execute files from untrusted and unknown sources.
- Remind users not to visit untrusted websites or follow links provided by untrusted or unknown sources.
- Evaluate read, write, and execute permissions on all newly installed software.
- Apply the Principle of Least Privilege to all systems and services.

REFERENCES:
Apple:
https://support.apple.com/en-us/HT213091
https://support.apple.com/en-us/HT213092
https://support.apple.com/en-us/HT213093

Security Week:
https://www.securityweek.com/apple-says-webkit-zero-day-hitting-ios-macos-devices

Bleeping Computer:
https://www.bleepingcomputer.com/news/security/apple-patches-new-zero-day-exploited-to-hack-iphones-ipads-macs/

CVE:

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-22620