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:
03/09/2021

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

OVERVIEW:
Multiple vulnerabilities have been discovered in Apple products, the most severe of which could allow for arbitrary code execution.

- macOS Big Sur is a desktop operating system for Macintosh computers.
- watchOS is a mobile operating system created & developed by Apple to be utilized by its Apple Watch product line.
- iOS is a mobile operating system created & developed by Apple to be utilized by its mobile devices such as the iPhone.
- Safari is a web browser available for macOS.
- iPadOS is a mobile operating system created & developed by Apple to be utilized by its iPad product line.

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:
There are no reports of these vulnerabilities being exploited in the wild.

SYSTEMS AFFECTED:

- watchOS versions prior to 7.3.2
- macOS versions prior to Big Sur 11.2.3
- iOS versions prior to 14.4.1
- iPadOS versions prior to 14.4.1
- Safari versions prior to 14.0.3

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. This vulnerability occurs when processing a specially crafted web content due to a memory corruption issue.

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:
The following actions should 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 un-trusted or unknown sources.
- Remind users not to visit untrusted websites or follow links provided by unknown or un-trusted sources.
- Apply the Principle of Least Privilege to all systems and services.

REFERENCES:
Apple:
https://support.apple.com/en-us/HT212220
https://support.apple.com/en-us/HT212221
https://support.apple.com/en-us/HT212222
https://support.apple.com/en-us/HT212223

CVE:
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-1844