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
https://www.cisa.gov/tlp
Sources may use TLP:WHITE when information carries minimal or no foreseeable risk of misuse, in accordance with applicable rules and procedures for public release. Subject to standard copyright rules, TLP:WHITE information may be distributed without restriction.

DATE(S) ISSUED:
09/14/2021

SUBJECT:
Multiple Vulnerabilities in Apple Products Could Allow for Remote Code Execution

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

- Safari is a graphical web browser developed by Apple, based on the WebKit engine.
- watchOS is the mobile operating system for Apple Watch and is based on the iOS operating system.
- 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 Big Sur is the 17th and current major release of macOS.
- macOS Catalina is the 16th major release of macOS.
- macOS Mojave is the 15th major release of macOS.

Successful exploitation of the most severe of these vulnerabilities could result in remote code execution in the context of the affected user.

THREAT INTELLIGENCE:
Apple has reported both CVE-2021-30858 and CVE-2021-30860 are being exploited in the wild.

SYSTEMS AFFECTED:
- watchOS versions before 7.6.2
- Safari versions before 14.1.2 (14611.3.10.1.7 on macOS Mojave and 15611.3.10.1.7 on macOS Catalina)
- iOS/iPadOS versions before 14.8
- macOS Big Sur versions before 11.6
- macOS Catalina without Security Update 2021-005

RISK:
Government:
- Large and medium government entities: **Medium**
- Small government entities: **Medium**

Businesses:

- Large and medium business entities: **Medium**
- Small business entities: **Medium**

Home users: Low

TECHNICAL SUMMARY:
Multiple vulnerabilities have been discovered in Apple Products, the most severe of which could allow for remote code execution in the context of the affected user. Details of these vulnerabilities are as follows:

- An integer overflow when processing PDF files within the CoreGraphics component. (CVE-2021-30860)
- A use-after-free error when processing HTML content in WebKit. (CVE-2021-30858)

Successful exploitation of the most severe of these vulnerabilities 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 nonprivileged 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/HT201222
https://support.apple.com/en-us/HT212804
https://support.apple.com/en-us/HT212805
https://support.apple.com/en-us/HT212806
https://support.apple.com/en-us/HT212807
https://support.apple.com/en-us/HT212808

CVE:
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-30858
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-30860

TLP: WHITE
https://www.cisa.gov/tlp
Sources may use TLP:WHITE when information carries minimal or no foreseeable risk of