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:
07/21/2021

SUBJECT:
Multiple Vulnerabilities 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.

- 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.
- 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.
- 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.
- tvOS is an operating system for fourth-generation Apple TV digital media player.

Successful exploitation of the most severe of these vulnerabilities could result in arbitrary code execution with kernel or root privileges.

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

SYSTEMS AFFECTED:
- macOS Big Sur versions prior to 11.5
- macOS Catalina prior to security update 2021-004
- macOS Mojave prior to security update 2021-005
- iOS and iPadOS versions prior to 14.7
- Safari versions prior to 14.1.2
- watchOS versions prior to 7.6
- tvOS versions prior to 14.7

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:

Multiple vulnerabilities have been discovered in Apple macOS/iOS, the most severe of which could allow for arbitrary code execution with kernel or root privileges. Details of these vulnerabilities are as follows:

- A shortcut may be able to bypass Internet permission requirements due to an input validation issue in ActionKit (CVE-2021-30763)
- A memory corruption issue in the AMD kernel may lead to arbitrary code execution with kernel privileges (CVE-2021-30805)
- Opening a maliciously crafted file may lead to unexpected AppKit termination or arbitrary code execution (CVE-2021-30790)
- A local attacker may be able to cause unexpected application termination or arbitrary code execution via Audio (CVE-2021-30781)
- A memory corruption issue within AVEVideoEncoder may lead to arbitrary code execution with kernel privileges (CVE-2021-30748)
- A malicious application may be able to gain root privileges due to a memory corruption issue in Bluetooth (CVE-2021-30672)
- Processing a maliciously crafted audio file may lead to arbitrary code execution due to a memory corruption issue in CoreAudio (CVE-2021-30775)
- Playing a malicious audio file may lead to unexpected application termination due to a logic issue with input validation in CoreAudio (CVE-2021-30776)
- Opening a maliciously crafted PDF file may lead to an unexpected application termination or arbitrary code execution due to a race condition in CoreGraphics (CVE-2021-30786)
- A malicious application may be able to gain root privileges via CoreServices, and a sandboxed process may be able to circumvent restrictions (CVE-2021-30772, CVE-2021-30783)
- A malicious application may be able to gain root privileges due to an injection issue in CoreStorage (CVE-2021-30777)
- Processing a maliciously crafted font file may lead to arbitrary code execution or process memory disclosure due to out-of-bounds reads in CoreText (CVE-2021-30789, CVE-2021-30733)
- A malicious application may be able to gain root privileges due to a logic issue within Crash Reporter (CVE-2021-30774)
- A malicious application may be able to gain root privileges due to an out-of-bounds write issue in CVMS (CVE-2021-30780)
- A sandboxed process may be able to circumvent sandbox restrictions due to a logic issue in dyld (CVE-2021-30768)
- A malicious application may be able to access Find My data due to a permissions issue (CVE-2021-30804)
- Processing a maliciously crafted font file may lead to arbitrary code execution due to integer and stack overflows in FontParser (CVE-2021-30760, CVE-2021-30759)
- Processing a maliciously crafted tiff file with FontParser may lead to a denial-of-service or potentially disclose memory contents (CVE-2021-30788)

- A malicious application may be able to access a user's recent Contacts due to a permissions issue in Identity Services (CVE-2021-30803)
- A malicious application may be able to bypass code signing checks due to a code signature validation issue in Identity Services (CVE-2021-30773)
- Processing maliciously crafted web content may lead to arbitrary code execution due to a use after free iddue in Image Processing (CVE-2021-30802)
- Processing a maliciously crafted image with may lead to arbitrary code execution due to a buffer overflow in ImageIO (CVE-2021-30779, CVE-2021-30785)
- An application may be able to cause unexpected system termination or write kernel memory due to an issue in Intel Graphics Driver (CVE-2021-30787)
- An application may be able to execute arbitrary code with kernel privileges due to an out-of-bounds write issue in Intel Graphics Driver (CVE-2021-30765, CVE-2021-30766)
- An unprivileged application may be able to capture USB devices due to an issue in IOUSBHostFamily (CVE-2021-30731)
- A local attacker may be able to execute code on the Apple T2 Security Chip due to multiple logic issues in IOKit (CVE-2021-30784)
- An application may be able to execute arbitrary code with kernel privileges due to logic issues in state management and double free issues in the kernel (CVE-2021-30703, CVE-2021-30793)
- A malicious attacker with arbitrary read and write capability may be able to bypass Pointer Authentication due to a kernel logic issue (CVE-2021-30769)
- An attacker that has already achieved kernel code execution may be able to bypass kernel memory mitigations due to a kernel logic issue (CVE-2021-30770)
- A malicious application may be able to bypass Privacy preferences due to entitlement issues in Kext Management (CVE-2021-30778)
- A malicious application or sandboxed process may be able to break out of its sandbox or restrictions due to environment sanitization and access restriction issues in LaunchServices (CVE-2021-30677, CVE-2021-30783)
- A remote attacker may be able to cause arbitrary code execution due to an issue in libxml2 (CVE-2021-3518)
- Multiple issues were found in libwebp (CVE-2018-25010, CVE-2018-25011, CVE-2018-25014, CVE-2020-36328, CVE-2020-36329, CVE-2020-36330, CVE-2020-36331)
- Processing a maliciously crafted image may lead to a denial of service due to a logic issue in Model I/O (CVE-2021-30796)
- Processing a maliciously crafted image may lead to arbitrary code execution due to an out-of-bounds write in Model I/O (CVE-2021-30792)
- Processing a maliciously crafted file may disclose user information due to an out-of-bounds read in Model I/O (CVE-2021-30791)
- A malicious application may be able to access restricted files due to an issue in Sandbox (CVE-2021-30782)
- A malicious application may be able to bypass certain Privacy preferences due to a logic issue in TCC (CVE-2021-30798)
- Processing maliciously crafted web content may lead to arbitrary code execution due to type confusion, use after free, and memory corruption issues in WebKit (CVE-2021-30758, CVE-2021-30795, CVE-2027-30797, CVE-2021-30799)
- Joining a malicious Wi-Fi network may result in a denial of service or arbitrary code execution (CVE-2021-30800)

RECOMMENDATIONS:
The following actions 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/HT212600
https://support.apple.com/en-us/HT212601
https://support.apple.com/en-us/HT212602
https://support.apple.com/en-us/HT212603
https://support.apple.com/en-us/HT212604
https://support.apple.com/en-us/HT212605
https://support.apple.com/en-us/HT212606

CVE:
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-25010
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-25011
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-25014
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-36328
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-36329
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-36330
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-36331
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-3518
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-30672
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-30677
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-30703
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-30731
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-30733
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-30748
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-30758
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-30759
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-30760
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-30763
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-30765
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-30766
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-30768
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-30769
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-30770
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-30772
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-30773

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-30774
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-30775
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-30776
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-30777
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-30778
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-30779
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-30780
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-30781
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-30782
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-30783
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-30784
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-30785
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-30786
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-30787
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-30788
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-30789
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-30790
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-30791
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-30792
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-30793
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-30795
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-30796
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-30797
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-30798
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-30799
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-30800
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-30802
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-30803
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-30804
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-30805