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:
01/27/2021
02/02/2021 - UPDATED
02/10/2021 - UPDATED

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.

- tvOS is an operating system for the fourth-generation Apple TV digital media player.
- watchOS is the mobile operating system for the Apple Watch and is based on the iOS operating system.
- iPadOS is the successor to iOS 12 and is a mobile operating system for iPads.
- iOS is a mobile operating system for mobile devices, including the iPhone, iPad, and iPod touch.
- Xcode is an integrated development environment (IDE) for macOS.

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.

February 2 – UPDATED OVERVIEW:

Several of the previous vulnerabilities have been found in macOS, an operating system for Apple desktops and laptops. Additional new vulnerabilities have also been discovered, the most severe of which could allow for arbitrary code execution with system privileges. An attacker could then install programs; view, change, or delete any data.

February 9 – UPDATED OVERVIEW:
Three additional vulnerabilities have been found in macOS which may allow for arbitrary code execution and privilege escalation.

THREAT INTELLIGENCE:
There are reports of the following vulnerabilities currently being actively exploited in the wild:

- CVE-2021-1782: iOS, iPadOS, tvOS, watchOS vulnerability that enables privilege escalation.
- CVE-2021-1870: WebKit vulnerability that enables arbitrary code execution.
- CVE-2021-1800: Xcode vulnerability that enables arbitrary file access.

February 2 – UPDATED THREAT INTELLIGENCE:
There are reports of the following vulnerabilities currently being actively exploited in the wild:
- CVE-2021-1782: macOS vulnerability that enables privilege escalation.
- CVE-2021-1870 and CVE-2021-1871: macOS vulnerability that enables arbitrary code execution.

SYSTEMS AFFECTED:
- iOS versions prior to iOS 14.4
- iPadOS versions prior to iPadOS 14.4
- tvOS versions prior to tvOS 14.4
- watchOS versions prior to watchOS 7.3
- Xcode versions prior to Xcode 12.4

February 2 – UPDATED SYSTEMS AFFECTED:
- macOS Big Sur versions up to 11.0.1
- macOS Catalina versions up to 10.15.7
- macOS Mojave versions up to 10.14.6

February 9 – UPDATED SYSTEMS AFFECTED:
- **macOS Big Sur versions up to 11.2**

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 iOS, iPadOS, tvOS, watchOS, and Xcode, the most severe of which could allow for arbitrary code execution. Details of these vulnerabilities are as follows:

iPadOS 14.4, iOS 14.4, tvOS 14.4 and watchOS 7.3
- A logic issue was addressed with improved restrictions (CVE-2021-1870, CVE-2021-1871)
- A race condition was addressed with improved locking. (CVE-2021-1782)

Xcode 12.4
- A path handling issue was addressed with improved validation. (CVE-2021-1800)

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.

February 2 – UPDATED TECHNICAL SUMMARY:
Multiple similar and new vulnerabilities have been discovered in macOS, the most severe of which could allow for arbitrary code execution with system privileges. Details of these vulnerabilities are as follows:

- Analytics: A remote attacker may be able to cause a denial of service (CVE-2021-1761)
- APFS: A local user may be able to read arbitrary files (CVE-2021-1797)
- CFNetwork Cache: Processing maliciously crafted web content may lead to arbitrary code execution (CVE-2020-27945)
- CoreAnimation: A malicious application could execute arbitrary code leading to compromise of user information (CVE-2021-1760)
- CoreAudio: Processing maliciously crafted web content may lead to code execution (CVE-2021-1747)
- CoreGraphics: Processing a maliciously crafted font file may lead to arbitrary code execution (CVE-2021-1776)
- CoreMedia: Processing a maliciously crafted image may lead to arbitrary code execution (CVE-2021-1759)
- CoreText:
    - Processing a maliciously crafted text file may lead to arbitrary code execution (CVE-2021-1772)
    - A remote attacker may be able to cause arbitrary code execution (CVE-2021-1792)
- Crash Reporter:
    - A remote attacker may be able to cause a denial of service (CVE-2021-1761)
    - A local attacker may be able to elevate their privileges (CVE-2021-1787)
    - A local user may be able to create or modify system files (CVE-2021-1786)
- Directory Utility: A malicious application may be able to access private information (CVE-2020-27937)
- Endpoint Security: A local attacker may be able to elevate their privileges (CVE-2021-1802)
- FairPlay: A malicious application may be able to disclose kernel memory (CVE-2021-1791)
- FontParser:
    - Processing a maliciously crafted font may lead to arbitrary code execution (CVE-2021-1790, CVE-2021-1775)
    - A remote attacker may be able to leak memory (CVE-2020-29608)
    - A remote attacker may be able to cause arbitrary code execution (CVE-2021-1758)
- ImageIO:
    - Processing a maliciously crafted image may lead to arbitrary code execution (CVE-2021-1783, CVE-2021-1741, CVE-2021-1743, CVE-2021-1736, CVE-2021-1785, CVE-2021-1742, CVE-2021-1746, CVE-2021-1754, CVE-2021-1774, CVE-2021-1777, CVE-2021-1793, CVE-2021-1737, CVE-2021-1738, CVE-2021-1744)
    - Processing a maliciously crafted image may lead to a denial of service (CVE-2021-1773, CVE-2021-1778)

    - A remote attacker may be able to cause unexpected application termination or arbitrary code execution (CVE-2021-1818)
- IOKit: An application may be able to execute arbitrary code with system privileges (CVE-2021-1779)
- IOSkywalkFamily: A local attacker may be able to elevate their privileges (CVE-2021-1757)
- Kernel:
    - An application may be able to execute arbitrary code with kernel privileges (CVE-2020-27904, CVE-2021-1750)
    - A remote attacker may be able to cause a denial of service (CVE-2021-1764)
    - A malicious application may be able to elevate privileges. Apple is aware of a report that this issue may have been actively exploited (CVE-2021-1782)
- Login Window: An attacker in a privileged network position may be able to bypass authentication policy (CVE-2020-29633)
- Messages: A user that is removed from an iMessage group could rejoin the group (CVE-2021-1771)
- Model I/O:
    - Processing a maliciously crafted USD file may lead to unexpected application termination or arbitrary code execution (CVE-2021-1762, CVE-2021-1763, CVE-2021-1745, CVE-2021-1768)
    - Processing a maliciously crafted file may lead to heap corruption (CVE-2020-29614)
    - Processing a maliciously crafted image may lead to heap corruption (CVE-2021-1767, CVE-2021-1753)
- NetFSFramework: Mounting a maliciously crafted Samba network share may lead to arbitrary code execution (CVE-2021-1751)
- OpenLDAP: A remote attacker may be able to cause a denial of service (CVE-2020-25709)
- Power Management: A malicious application may be able to elevate privileges (CVE-2020-27938)
- Screen Sharing: Multiple issues in pcre (CVE-2019-20838, CVE-2020-14155)
- SQLite: Multiple issues in SQLite (CVE-2020-15358)
- Swift: A malicious attacker with arbitrary read and write capability may be able to bypass Pointer Authentication (CVE-2021-1769)
- WebKit:
    - Maliciously crafted web content may violate iframe sandboxing policy (CVE-2021-1765, CVE-2021-1801)
    - Processing maliciously crafted web content may lead to arbitrary code execution (CVE-2021-1789)
    - A remote attacker may be able to cause arbitrary code execution. Apple is aware of a report that this issue may have been actively exploited. (CVE-2021-1871, CVE-2021-1870)
- WebRTC: A malicious website may be able to access restricted ports on arbitrary servers (CVE-2021-1799)

February 9 – UPDATED TECHNICAL SUMMARY:
Three additional vulnerabilities have been found in macOS which may allow for arbitrary code execution and privilege escalation. Details of these vulnerabilities are as follows:

- ***Intel graphics driver***

    - ***An out-of-bounds write was addressed with improved input validation. (CVE-2021-1805)***
    - ***A race condition was addressed with additional validation. (CVE-2021-1806)***
- ***Sudo***
    - ***A privilege escalation vulnerability within sudo (CVE-2021-3156)***

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/HT212146
https://support.apple.com/en-us/HT212149
https://support.apple.com/en-us/HT212148
https://support.apple.com/en-us/HT212153

CVE:
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-1782
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-1800
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-1870
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-1871

February 2 - UPDATED REFERENCES:
Apple:
https://support.apple.com/en-us/HT212147

CVE:
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-14155
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-15358
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-20838
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-25709
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-27904
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-27937
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-27938
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-27945
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-29608
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-29614
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-29633

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-1736
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-1737
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-1738
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-1741
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-1742
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-1743
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-1744
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-1745
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-1746
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-1747
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-1750
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-1751
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-1753
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-1754
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-1757
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-1758
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-1759
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-1760
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-1761
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-1762
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-1763
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-1764
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-1765
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-1766
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-1767
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-1768
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-1769
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-1771
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-1772
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-1773
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-1774
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-1775
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-1776
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-1777
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-1778
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-1779
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-1783
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-1785
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-1786
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-1787
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-1788
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-1789
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-1790
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-1791
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-1792
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-1793
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-1797
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-1799
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-1801
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-1802
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-1818

February 9 - UPDATED REFERENCES:
Apple:
https://support.apple.com/en-us/HT212177

CVE:
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-1805
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-1806
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-3156