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:
01/27/2022

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.
- macOS Monterey is the 18th and current major release of macOS.
- macOS Big Sur is the 17th release of macOS.
- macOS Catalina is the 16th major release of macOS
- watchOS is the mobile operating system for Apple Watch and is based on the iOS operating system.
- tvOS is an operating system for fourth-generation Apple TV digital media player.
- Safari is a graphical web browser developed by Apple.

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.

THREAT INTELLIGENCE:
Apple is aware of a report that CVE-2022-22587 may have been actively exploited.

SYSTEMS AFFECTED:
- iOS and iPadOS prior to 15.3
- macOS Monterey prior to 12.2
- macOS Big Sur prior to 11.6.3
- macOS Catalina prior to security update 2022-001
- watchOS prior to 8.4
- tvOS prior to 15.3
- Safari prior to 15.3

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 Products, the most severe of which could allow for arbitrary code execution in the context of the affected user. Details of these vulnerabilities are as follows:

iOS and iPadOS 15.3
- An application may be able to access a user's files. (CVE-2022-22585)
- A malicious application may be able to execute arbitrary code with kernel privileges. Apple is aware of a report that this issue may have been actively exploited. (CVE-2022-22587)
- A malicious application may be able to execute arbitrary code with kernel privileges (CVE-2022-22593)
- Processing a maliciously crafted STL file may lead to unexpected application termination or arbitrary code execution. (CVE-2022-22579)
- Processing a maliciously crafted mail message may lead to running arbitrary JavaScript. (CVE-2022-22589)
- Processing maliciously crafted web content may lead to arbitrary code execution. (CVE-2022-22590)
- Processing maliciously crafted web content may prevent Content Security Policy from being enforced. (CVE-2022-22592)
- A website may be able to track sensitive user information. (CVE-2022-22594)

MacOS Monterey 12.2
- A malicious application may be able to execute arbitrary code with kernel privileges. An out-of-bounds write issue was addressed with improved bounds checking. (CVE-2022-22586)
- Processing a maliciously crafted file may lead to arbitrary code execution. A memory corruption issue was addressed with improved validation. (CVE-2022-22584)
- A malicious application may be able to gain root privileges. A logic issue was addressed with improved validation. (CVE-2022-22578)
- An application may be able to access a user's files. An issue existed within the path validation logic for symlinks. This issue was addressed with improved path sanitization. (CVE-2022-22585)
- A malicious application may be able to execute arbitrary code with kernel privileges. A memory corruption issue was addressed with improved memory handling. (CVE-2022-22591)
- A malicious application may be able to execute arbitrary code with kernel privileges. Apple is aware of a report that this issue may have been actively exploited. A memory corruption issue was addressed with improved input validation. (CVE-2022-22587)

- A malicious application may be able to execute arbitrary code with kernel privileges. A buffer overflow issue was addressed with improved memory handling. (CVE-2022-22593)
- Processing a maliciously crafted STL file may lead to unexpected application termination or arbitrary code execution. An information disclosure issue was addressed with improved state management. (CVE-2022-22579)
- An application may be able to access restricted files. A permissions issue was addressed with improved validation. (CVE-2022-22583)
- Processing a maliciously crafted mail message may lead to running arbitrary JavaScript. A validation issue was addressed with improved input sanitization. (CVE-2022-22589)
- Processing maliciously crafted web content may lead to arbitrary code execution. A use after free issue was addressed with improved memory management.. (CVE-2022-22590)
- Processing maliciously crafted web content may prevent Content Security Policy from being enforced. A logic issue was addressed with improved state management. (CVE-2022-22592)
- A website may be able to track sensitive user information. A cross-origin issue in the IndexDB API was addressed with improved input validation. (CVE-2022-22594)

MacOS Big Sur 11.6.3

- Parsing a maliciously crafted audio file may lead to disclosure of user information. (CVE-2021-30960)
- An application may be able to access a user's files. (CVE-2022-22585)
- A malicious application may be able to execute arbitrary code with kernel privileges. Apple is aware of a report that this issue may have been actively exploited. (CVE-2022-22587)
- A malicious application may be able to execute arbitrary code with kernel privileges. (CVE-2022-22593)
- Processing a maliciously crafted STL file may lead to unexpected application termination or arbitrary code execution. (CVE-2022-22579)
- An application may be able to access restricted files. (CVE-2022-22583)
- A malicious application may be able to bypass certain Privacy preferences. (CVE-2021-30972)

MacOS Catalina Security Update 2022-001

- A malicious application may be able to execute arbitrary code with kernel privileges. (CVE-2022-22593)
- Processing a maliciously crafted STL file may lead to unexpected application termination or arbitrary code execution. (CVE-2022-22579)
- An application may be able to access restricted files. (CVE-2022-22583)
- A malicious application may be able to bypass certain Privacy preferences. (CVE-2021-30946 & CVE-2021-30972)

WatchOS 8.4

- Processing a maliciously crafted file may lead to arbitrary code execution. (CVE-2022-22584)
- A malicious application may be able to gain root privileges. (CVE-2022-22578)
- An application may be able to access a user's files. (CVE-2022-22585)

- A malicious application may be able to execute arbitrary code with kernel privileges. (CVE-2022-22593)
- Processing maliciously crafted web content may lead to arbitrary code execution. (CVE-2022-22590)
- Processing maliciously crafted web content may prevent Content Security Policy from being enforced. (CVE-2022-22592)
- Processing a maliciously crafted mail message may lead to running arbitrary JavaScript. (CVE-2022-22589)
- A website may be able to track sensitive user information. (CVE-2022-22594)

tvOS 15.3

- Processing a maliciously crafted file may lead to arbitrary code execution. (CVE-2022-22584)
- A malicious application may be able to gain root privileges. (CVE-2022-22578)
- An application may be able to access a user's files. (CVE-2022-22585)
- A malicious application may be able to execute arbitrary code with kernel privileges. (CVE-2022-22593)
- Processing a maliciously crafted STL file may lead to unexpected application termination or arbitrary code execution. (CVE-2022-22579)
- Processing maliciously crafted web content may lead to arbitrary code execution. (CVE-2022-22590)
- Processing maliciously crafted web content may prevent Content Security Policy from being enforced. (CVE-2022-22592)
- Processing a maliciously crafted mail message may lead to running arbitrary JavaScript. (CVE-2022-22589)
- A website may be able to track sensitive user information. (CVE-2022-22594)

Safari 15.3

- Processing maliciously crafted web content may lead to arbitrary code execution. (CVE-2022-22590)
- Processing maliciously crafted web content may prevent Content Security Policy from being enforced. (CVE-2022-22592)
- Processing a maliciously crafted mail message may lead to running arbitrary JavaScript. (CVE-2022-22589)
- A website may be able to track sensitive user information. (CVE-2022-22594)

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 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/HT213053
https://support.apple.com/en-us/HT213054
https://support.apple.com/en-us/HT213055
https://support.apple.com/en-us/HT213056
https://support.apple.com/en-us/HT213057
https://support.apple.com/en-us/HT213058
https://support.apple.com/en-us/HT213059

CVE:

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-30946
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-30960
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-30972
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-22578
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-22579
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-22583
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-22584
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-22585
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-22586
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-22587
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-22589
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-22590
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-22591
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-22592
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-22593
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-22594