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:

10/27/2021

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.
- 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.

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:

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

SYSTEMS AFFECTED:

- iOS and iPadOS prior to 15.1
- iOS and iPadOS prior to 14.8.1
- macOS Monterey prior to 12.0.1
- macOS Big Sur prior to 11.6.1
- macOS Catalina prior to security update 2021-007
- watchOS prior to 8.1
- tvOS prior to 15.1

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:

- An integer overflow was addressed through improved input validation. (CVE-2021-30907)
- A memory corruption issue existed in the processing of ICC profiles. This issue was addressed with improved input validation. (CVE-2021-30917)
- This issue was addressed with improved checks. (CVE-2021-30903, CVE-2021-30906)
- An out-of-bounds read was addressed with improved bounds checking. (CVE-2021-30905, CVE-2021-30910, CVE-2021-30911)
- An out-of-bounds write was addressed with improved input validation. (CVE-2021-30919)
- An input validation issue was addressed with improved memory handling. (CVE-2021-30881)
- An out-of-bounds write issue was addressed with improved bounds checking. (CVE-2021-30900)
- A memory corruption issue was addressed with improved input validation. (CVE-2021-30894, CVE-2021-30914)
- A use after free issue was addressed with improved memory management. (CVE-2021-30886, CVE-2021-30902)
- A memory corruption issue was addressed with improved memory handling. (CVE-2021-30909, CVE-2021-30916)
- A lock screen issue allowed access to contacts on a locked device. This issue was addressed with improved state management. (CVE-2021-30875)
- A logic issue was addressed with improved state management. (CVE-2021-30890, CVE-2021-30915)
- A logic issue was addressed with improved restrictions. (CVE-2021-30887)
- An information leakage issue was addressed. (CVE-2021-30888)
- A buffer overflow issue was addressed with improved memory handling. (CVE-2021-30889)
- A memory corruption issue was addressed with improved memory handling. (CVE-2021-30883)
- A Lock Screen issue was addressed with improved state management. (CVE-2021-30918)
- A logic issue was addressed with improved state management. (CVE-2021-30873)
- An out-of-bounds read was addressed with improved bounds checking. (CVE-2021-30876, CVE-2021-30879, CVE-2021-30877, CVE-2021-30880)
- A race condition was addressed with improved state handling. (CVE-2021-30899)
- A logic issue was addressed with improved restrictions. (CVE-2021-30895)

- A logic issue was addressed with improved restrictions. (CVE-2021-30896)
- A memory corruption issue was addressed with improved state management. (CVE-2021-30824)
- Multiple out-of-bounds write issues were addressed with improved bounds checking. (CVE-2021-30901)
- A memory corruption issue was addressed with improved memory handling. (CVE-2021-30821)
- A logic issue was addressed with improved state management. (CVE-2021-30864)
- This issue was addressed with improved checks. (CVE-2021-30813)
- A permissions issue was addressed with improved validation. (CVE-2021-30920)
- A race condition was addressed with improved locking. (CVE-2021-30868)
- The issue was addressed with improved permissions logic. (CVE-2021-30912, CVE-2021-30913)
- A logic issue was addressed with improved restrictions. (CVE-2021-30823)
- A logic issue was addressed with improved state management. (CVE-2021-30861)
- An authentication issue was addressed with improved state management. (CVE-2021-30908)
- This issue was addressed with improved checks. (CVE-2021-30833)
- An inherited permissions issue was addressed with additional restrictions. (CVE-2021-30892)

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/HT212868
https://support.apple.com/en-us/HT212869
https://support.apple.com/en-us/HT212872
https://support.apple.com/en-us/HT212871
https://support.apple.com/en-us/HT212874
https://support.apple.com/en-us/HT212867
https://support.apple.com/en-us/HT212876

CVE:
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-30813
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-30821
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-30823
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-30824
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-30833
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-30861
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-30864
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-30868
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-30873
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-30875
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-30876
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-30877
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-30879
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-30880
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-30881
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-30883
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-30886
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-30887
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-30888
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-30889
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-30890
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-30892
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-30894
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-30895
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-30896
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-30899
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-30900
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-30901
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-30902
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-30903
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-30905
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-30906
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-30907
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-30908
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-30909
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-30910
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-30911
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-30912
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-30913
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-30914
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-30915
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-30916
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-30917
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-30918
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-30919
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-30920