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:

05/04/2021

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.

- macOS Big Sur is the 17th and current major release of macOS.
- 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.
- watchOS is the mobile operating system for the Apple Watch and is based on the iOS operating system.

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 reports that these vulnerabilities are being actively exploited in the wild.

SYSTEMS AFFECTED:

- macOS Big Sur prior to version 11.3.1
- iOS prior to version 14.5.1
- iOS prior to version 12.5.3
- iPadOS prior to version 14.5.1
- watchOS prior to version 7.4.1

RISK:

Government:

- Large and medium government entities: **High**
- Small government entities: **High**

Businesses:

- Large and medium business entities: **High**

- Small business entities: **High**

Home users: Low

TECHNICAL SUMMARY:

Multiple vulnerabilities have been discovered in Apple Products, the most severe of which could allow for arbitrary code execution. Details of these vulnerabilities are as follows:

iOS 14.5.1 and iPadOS 14.5.1

- A memory corruption issue was addressed with improved state management. (CVE-2021-30665)
- An integer overflow was addressed with improved input validation. (CVE-2021-30663)

iOS 12.5.3

- A buffer overflow issue was addressed with improved memory handling. (CVE-2021-30666)
- A memory corruption issue was addressed with improved state management. (CVE-2021-30665)
- An integer overflow was addressed with improved input validation. (CVE-2021-30663)
- A use after free issue was addressed with improved memory management. (CVE-2021-30661)

macOS Big Sur 11.3.1

- A memory corruption issue was addressed with improved state management. (CVE-2021-30665)
- An integer overflow was addressed with improved input validation. (CVE-2021-30663)

watchOS 7.4.1

- A memory corruption issue was addressed with improved state management. (CVE-2021-30665)

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/HT212335
https://support.apple.com/en-us/HT212336
https://support.apple.com/en-us/HT212339
https://support.apple.com/en-us/HT212341

CVE:
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-30661
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-30663
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-30665
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-30666