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

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.

THREAT INTELLIGENCE:
These 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.

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

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.

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