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:
09/23/2021

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.
- macOS Catalina is the 16th major release of macOS.

Successful exploitation of the most severe of these vulnerabilities could result in arbitrary code execution with kernel privileges.

THREAT INTELLIGENCE:
Apple has reported that all three vulnerabilities below have been seen in the wild. (CVE-2021-30860, CVE-2021-30869, CVE-2021-30858)

SYSTEMS AFFECTED:
- iOS prior to 12.5.5
- macOS Catalina prior to Security Update 2021-006

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 with kernel privileges. Details of these vulnerabilities are as follows:

iOS

- An integer overflow was addressed with improved input validation, which could lead to arbitrary code execution. (CVE-2021-30860)
- A use after free issue was addressed with improved memory management, which could lead to arbitrary code execution. (CVE-2021-30858)
- A type confusion issue was addressed with improved state handling, which could lead to arbitrary code execution. (CVE-2021-30869)

macOS Catalina

- A type confusion issue was addressed with improved state handling, which could allow for arbitrary code execution with kernel privileges. (CVE-2021-30869)

Successful exploitation of the most severe of these vulnerabilities could result in arbitrary code execution with kernel privileges. 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/HT212824
https://support.apple.com/en-us/HT212825

CVE:

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-30858
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-30860
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-30869

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.