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:

07/27/2021

SUBJECT:

A Vulnerability in macOS Big Sur, iOS and iPadOS Could Allow for Arbitrary Code Execution

OVERVIEW:

A vulnerability has been discovered in macOS Big Sur, iOS and iPadOS, 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 Big Sur is the 17th and current major release of macOS.

Successful exploitation of this vulnerability could allow an attacker to execute arbitrary code with kernel privileges to take full control over a device.

THREAT INTELLIGENCE:

Apple is aware of a report that this issue may have been actively exploited to plant malware on vulnerable devices. (CVE-2021-30807)

SYSTEMS AFFECTED:

- iOS prior to version 14.7.1
- iPadOS prior to version 14.7.1
- macOS Big Sur prior to version 11.5.1

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:

A vulnerability has been discovered in macOS Big Sur, iOS and iPadOS that could allow for arbitrary code execution. This vulnerability occurs due to a memory corruption issue in IOMobileFrameBuffer that was addressed with improved memory handling. Successful exploitation of this vulnerability could result in arbitrary code execution with kernel privileges to take full control over a device.

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/HT212622
https://support.apple.com/en-us/HT212623

CVE:
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-30807

Security Affairs:
https://securityaffairs.co/wordpress/120576/security/apple-cve-2021-30807-zero-day.html

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.