*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**
**www.cisa.gov/tlp**
**Information may be distributed without restriction, subject to standard copyright rules.**

**DATE(S) ISSUED:**
04/01/2022

**SUBJECT:**
Multiple Vulnerabilities Vulnerability in Apple Products Could Allow for Local Code Execution

**OVERVIEW:**
Multiple vulnerabilities have been discovered in Apple products, the most severe of which could allow for local code execution. Successful exploitation of the most severe vulnerability could allow an attacker to execute code in the context of the kernel. Malicious actors with administrative access may be able to install programs; view, change, or delete data; or create new accounts with full user rights.

**THREAT INTELLIGENCE:**
Apple indicated that this issue may have been actively exploited.

**SYSTEMS AFFECTED:**

- iOS 15.4.1 and older
- iPadOS 15.4.1 and older
- macOS Monterey 12.3.1 and older

**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 local code execution. Successful exploitation of the most severe vulnerability could allow an attacker to execute code in the context of the kernel. Details of these vulnerabilities are as follows:

- An out-of-bound write vulnerability in AppleAVD which could allow for execute arbitrary code with kernel privileges (CVE-2022-22675)
- An out-of-bound read vulnerability in Intel Graphics Drivers which could allow for disclosure of kernel memory (CVE-2022-22674)

Malicious actors with administrative access may be able to install programs; view, change, or delete data; or create new accounts with full user rights.

**RECOMMENDATIONS:**
We recommend the following actions be taken:

- Apply updates provided by Apple to vulnerable systems immediately after appropriate testing.
- Remind users not to visit un-trusted websites or follow links provided by unknown or un-trusted sources.
- Inform and educate users regarding the threats posed by hypertext links contained in emails or attachments especially from un-trusted sources.

Apply the Principle of Least Privilege to all systems and services.

**REFERENCES:**

**Apple:**https://support.apple.com/en-us/HT213220https://support.apple.com/en-us/HT213219

**CVE:**https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-22675
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-22674