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:
091/01/2022

SUBJECT:
A Vulnerability in iOS Could Allow For Arbitrary Code Execution (CVE-2022-32893)

OVERVIEW:
A vulnerability has been discovered in Apple Products which could allow for arbitrary code execution. iOS is a mobile operating system created and developed by Apple Inc. exclusively for its hardware. Successful exploitation could allow the attacker to execute arbitrary code in context of the application. Depending on the permission associated with the application running the exploit, an attacker could then install programs; view, change, or delete data.Overview here

THREAT INTELLIGENCE:
Apple indicated that this vulnerability may be actively exploited in the wild.

SYSTEMS AFFECTED:

- iOS versions prior to iOS 12.5.6

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: Medium

TECHNICAL SUMMARY:

Tactic: *Execution* (TA0002):

Technique: *Native API* (T1106):

A vulnerability has been discovered in Apple Products which could allow for arbitrary code execution. iOS is a mobile operating system created and developed by Apple Inc. exclusively for its hardware. The vulnerability is an out-of-bound write vulnerability in WebKit. Successful exploitation could allow the attacker to execute arbitrary code in the context of the application. Depending on the permission associated with the application running the exploit, an attacker could then install programs; view, change, or delete data. (CVE-2022-32893)

RECOMMENDATIONS:
We recommend the following actions be taken:

- Apply appropriate patches provided by Atlassian to vulnerable systems, immediately after appropriate testing. (**M1051: Update Software**)
    - **Safeguard 7.1: Establish and Maintain a Vulnerability Management Process**: Establish and maintain a documented vulnerability management process for enterprise assets. Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.
    - **Safeguard 7.4: Perform Automated Application Patch Management:** Perform application updates on enterprise assets through automated patch management on a monthly, or more frequent, basis.
    - **Safeguard 7.5: Perform Automated Vulnerability Scans of Internal Enterprise Assets:** Perform automated vulnerability scans of internal enterprise assets on a quarterly, or more frequent, basis. Conduct both authenticated and unauthenticated scans, using a SCAP-compliant vulnerability scanning tool.
- Block execution of code on a system through application control, and/or script blocking. (**M1038** : **Execution Prevention**)
    - **Safeguard 2.5 : Allowlist Authorized Software:** Use technical controls, such as application allowlisting, to ensure that only authorized software can execute or be accessed. Reassess bi-annually, or more frequently.
    - **Safeguard 2.6 : Allowlist Authorized Libraries:** Use technical controls to ensure that only authorized software libraries, such as specific .dll, .ocx, .so, etc., files, are allowed to load into a system process. Block unauthorized libraries from loading into a system process. Reassess bi-annually, or more frequently.
    - **Safeguard 2.7 : Allowlist Authorized Scripts:** Use technical controls, such as digital signatures and version control, to ensure that only authorized scripts, such as specific .ps1, .py, etc., files, are allowed to execute. Block unauthorized scripts from executing. Reassess bi-annually, or more frequently.

REFERENCES:

Apple:

https://support.apple.com/en-us/HT213428

CVE:

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-32893