*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:**
05/14/2019

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

**OVERVIEW:**
Multiple vulnerabilities have been discovered in watchOS, Safari, tvOS, iOS, Mojave, High Sierra and Sierra. The most severe of these vulnerabilities could allow for arbitrary code execution.

- watchOS is the mobile operating system for the Apple Watch and is based on the iOS operating system.
- Safari is a web browser available for OS X.
- tvOS is an operating system for the fourth-generation Apple TV digital media player.
- iOS is a mobile operating system for mobile devices, including the iPhone, iPad, and iPod touch.
- Mojave
- High Sierra is a desktop and server operating system for Macintosh computers.
- Sierra is a desktop and server operating system for Macintosh computers.

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 privileges associated with the user, an attacker could then install programs; view, change, or delete data; or create new accounts with full user rights.

**THREAT INTELLIGENCE:**
There are currently no reports of these vulnerabilities being exploited in the wild.

**SYSTEMS AFFECTED:**

- watchOS versions prior to 5.2.1
- Safari versions prior to 12.1.1
- Apple TV Software 7.3
- tvOS versions prior to 12.3
- iOS versions prior to 12.3
- macOS Mojave 10.14.5, Security Update 2019-003 High Sierra, Security Update 2019-003 Sierra

**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 watchOS, Safari, tvOS, iOS, Mojave, High Sierra and Sierra. The most severe of these vulnerabilities could allow for arbitrary code execution. Details of these vulnerabilities are as follows:

- A buffer overflow issue was addressed with improved memory handling. (CVE-2019-6224)
- A buffer overflow was addressed with improved bounds checking. (CVE-2019-6213)
- A cross-site scripting issue existed in Safari. This issue was addressed with improved URL validation. (CVE-2019-6228)
- A denial of service issue was addressed with improved validation. (CVE-2019-6219)
- A logic issue was addressed with improved validation. (CVE-2019-6229)
- A memory consumption issue was addressed with improved memory handling. (CVE-2018-4452)
- A memory corruption issues were addressed with improved input validation. (CVE-2018-20346, CVE-2018-20505, CVE-2018-20506)
- A memory corruption issue was addressed with improved lock state checking. (CVE-2019-6205)
- An issue existed with autofill resuming after it was canceled. The issue was addressed with improved state management. (CVE-2019-6206)
- An out-of-bounds read issue existed that led to the disclosure of kernel memory. This was addressed with improved input validation. (CVE-2019-6209)
- Multiple memory corruption issues were addressed with improved input validation. (CVE-2019-6210, CVE-2019-6218)
- Multiple memory corruption issues were addressed with improved memory handling. (CVE-2019-6212, CVE-2019-6216, CVE-2019-6217, CVE-2019-6226)
- Multiple memory corruption issues were addressed with improved memory handling. (CVE-2019-6227, CVE-2019-6233, CVE-2019-6234)
- Multiple memory corruption issues were addressed with improved state management. (CVE-2018-4467, CVE-2019-6211)
- Multiple memory corruption issues were addressed with improved validation. (CVE-2019-6225, CVE-2019-6235)
- Multiple memory initialization issues were addressed with improved memory handling. (CVE-2019-6208, CVE-2019-6230)
- Multiple out-of-bounds read was addressed with improved bounds checking. (CVE-2019-6202, CVE-2019-6221, CVE-2019-6231)
- Multiple out-of-bounds read was addressed with improved input validation. (CVE-2019-6200, CVE-2019-6220)
- Multiple type confusion issues were addressed with improved memory handling. (CVE-2019-6214, CVE-2019-6215)

**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 non-privileged user (one without administrative privileges) to diminish the effects of a successful attack.
- Remind users not to download, accept, or execute files from un-trusted or unknown sources.
- Remind users not to visit untrusted websites or follow links provided by unknown or un-trusted sources.
- Apply the Principle of Least Privilege to all systems and services.

**REFERENCES:**

**Apple:**

https://support.apple.com/en-us/HT210118
https://support.apple.com/en-us/HT210119
https://support.apple.com/en-us/HT210120
https://support.apple.com/en-us/HT210121
https://support.apple.com/en-us/HT210122
https://support.apple.com/en-us/HT210123

**CVE:**

http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-4452
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-4467
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-20346
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-20505
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-20506
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-6200
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-6202
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-6205
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-6206
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-6208
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-6209
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-6210
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-6211
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-6212
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-6213
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-6214
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-6215
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-6216
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-6217
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-6218
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-6219
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-6220
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-6221
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-6224
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-6225
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-6226
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-6227
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-6228
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-6229
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-6230
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-6231

http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-6233
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-6234
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-6235

**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/**

**Greg Nohra**
Enterprise Security Architect
MS Department of Information Technology Services
601-432-8009 | www.its.ms.gov