

*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:**

07/22/2019

**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.
- macOS Mojave is a desktop and server operating system for Macintosh computers.
- 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 5.3
- Safari versions prior to 12.1.2
- tvOS versions prior to 12.4
- iOS versions prior to 12.4
- macOS Mojave 10.14.6, Security Update 2019-004 High Sierra, Security Update 2019-004 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 denial of service issue was addressed with improved validation. (CVE-2019-8665)
- A logic issue existed in the answering of phone calls. The issue was addressed with improved state management. (CVE-2019-8699)
- A logic issue existed in the handling of document loads. This issue was addressed with improved state management. (CVE-2019-8690)
- A logic issue existed in the handling of synchronous page loads. This issue was addressed with improved state management. (CVE-2019-8649)
- A logic issue was addressed with improved state management. (CVE-2019-8658)
- A stack overflow was addressed with improved input validation. (CVE-2019-13118)
- A validation issue existed in the entitlement verification. This issue was addressed with improved validation of the process entitlement. (CVE-2019-8698)
- Multiple inconsistent user interface issues were addressed with improved state management. (CVE-2019-8667, CVE-2019-8670)
- Multiple memory corruption issues were addressed with improved input validation. (CVE-2018-19860, CVE-2019-8648, CVE-2019-8660)
- Multiple memory corruption issues were addressed with improved memory handling. (CVE-2019-8644, CVE-2019-8666, CVE-2019-8669, CVE-2019-8671, CVE-2019-8672, CVE-2019-8673, CVE-2019-8676, CVE-2019-8677, CVE-2019-8678, CVE-2019-8679, CVE-2019-8680, CVE-2019-8681, CVE-2019-8683, CVE-2019-8684, CVE-2019-8685, CVE-2019-8686, CVE-2019-8687, CVE-2019-8688, CVE-2019-8689, CVE-2019-8694, CVE-2019-8695, CVE-2019-8697)
- Multiple out-of-bounds read was addressed with improved input validation. (CVE-2019-8624, CVE-2019-8641, CVE-2019-8646, CVE-2019-8657)
- Multiple use after free issues were addressed with improved memory management. (CVE-2019-8647, CVE-2019-8661)
- Multiple validation issues were addressed with improved input sanitization. (CVE-2019-8691, CVE-2019-8692, CVE-2019-8693)
- Issue was addressed with improved checks. (CVE-2019-8659, CVE-2019-8662, CVE-2019-8663)
- Issue was addressed with improved UI handling. (CVE-2019-8682)
- Issue was addressed with improved checks to prevent unauthorized actions. (CVE-2018-16860)
- This was addressed with additional checks by Gatekeeper on files mounted through a network share. (CVE-2019-8656)

**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/HT210346>

<https://support.apple.com/en-us/HT210348>

<https://support.apple.com/en-us/HT210351>

<https://support.apple.com/en-us/HT210353>

<https://support.apple.com/en-us/HT210355>

### CVE:

<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-16860>

<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-19860>

<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-8624>

<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-8641>

<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-8644>

<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-8646>

<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-8647>

<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-8648>

<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-8649>

<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-8656>

<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-8657>

<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-8658>

<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-8659>

<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-8660>

<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-8661>

<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-8662>

<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-8663>

<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-8665>

<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-8666>

<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-8667>

<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-8669>

<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-8670>

<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-8671>

<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-8672>

<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-8673>

<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-8676>

<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-8677>

<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-8678>

<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-8679>

<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-8680>

<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-8681>

<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-8682>  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-8683>  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-8684>  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-8685>  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-8686>  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-8687>  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-8688>  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-8689>  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-8690>  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-8691>  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-8692>  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-8693>  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-8694>  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-8695>  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-8697>  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-8698>  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-8699>  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-13118>

**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/>

This message and attachments may contain confidential information. If it appears that this message was sent to you by mistake, any retention, dissemination, distribution or copying of this message and attachments is strictly prohibited. Please notify the sender immediately and permanently delete the message and any attachments.

**Chris Watts**

Security Operations Analyst  
MS Department of Information Technology Services  
601-432-8201 | [www.its.ms.gov](http://www.its.ms.gov)



DISCLAIMER: This email and any files transmitted with it are confidential and intended solely for the use of the individual or entity to whom they are addressed. If you have received this email in error please notify the system manager. This message contains confidential information and is intended only for the individual named. If you are not the named addressee you should not disseminate, distribute or copy this e-mail. Please notify the sender immediately by e-mail if you have received this e-mail by mistake and delete this e-mail from your system. If you are not the intended recipient you are notified that disclosing, copying, distributing or taking any action in reliance on the contents of this information is strictly prohibited