TLP: WHITE
MS-ISAC CYBERSECURITY ADVISORY

MS-ISAC ADVISORY NUMBER: 2019-074

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:

We recommend the following actions 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

24×7 Security Operations Center
Multi-State Information Sharing and Analysis Center (MS-ISAC)
Elections Infrastructure Information Sharing and Analysis Center (EI-ISAC)
31 Tech Valley Drive
East Greenbush, NY 12061
SOC@cisecurity.org - 1-866-787-4722

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/