TLP: WHITE
MS-ISAC CYBERSECURITY ADVISORY

MS-ISAC ADVISORY NUMBER: 2018-060

DATE(S) ISSUED: 06/04/2018

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

OVERVIEW:
Multiple vulnerabilities have been discovered in iCloud for Windows, Safari, macOS High Sierra, Sierra, and El Capitan, iOS, watchOS, tvOS and iTunes. The most severe of these vulnerabilities could allow for arbitrary code execution.

- iCloud is a cloud storage service.
- Safari is a web browser available for macOS.
- macOS High Sierra is a desktop and server operating system for Macintosh computers.
- macOS Sierra is a desktop and server operating system for Macintosh computers.
- macOS El Capitan is a desktop and server operating system for Macintosh computers.
- iOS is a mobile operating system for mobile devices, including the iPhone, iPad, and iPod touch.
- watchOS is the mobile operating system for the Apple Watch and is based on the iOS operating system.
- tvOS is an operating system for the fourth-generation Apple TV digital media player.
- iTunes is a media player, media library, online radio broadcaster, and mobile device management application developed by Apple.

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:

- iCloud for Windows versions prior to Version 7.5
- Safari versions prior to 11.1.1
- macOS High Sierra versions prior to 10.13.5, Security Update 2018-003 Sierra, and Security Update 2018-003 El Capitan
- iOS versions prior to 11.4
- watchOS versions prior to 4.3.1
- tvOS versions prior to 11.4
- iTunes versions prior to 12.7.5 for Windows

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: Low

TECHNICAL SUMMARY:
Multiple vulnerabilities have been discovered in iCloud, Safari, macOS High Sierra, Sierra, and El Capitan, iOS, watchOS, tvOS and iTunes. 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-2018-4199)
- A buffer overflow was addressed with improved bounds checking. (CVE-2018-4241, CVE-2018-4243)
- A buffer overflow was addressed with improved size validation. (CVE-2018-4215)
- A device configuration issue was addressed with an updated configuration. (CVE-2018-4251)
- A logic issue was addressed with improved validation. (CVE-2018-4237)
- A memory corruption issues were addressed with improved memory handling. (CVE-2018-4201, CVE-2018-4218, CVE-2018-4233)
- A memory corruption issue was addressed with improved error handling. (CVE-2018-4206)
- A memory corruption issue was addressed with improved input validation. (CVE-2018-4214)
- A memory corruption issue was addressed with improved state management. (CVE-2018-4200)
- A memory corruption issue was addressed with improved validation. (CVE-2018-4211)
- A memory corruption vulnerability was addressed with improved locking. (CVE-2018-4242)
- An information disclosure issue existed in Accessibility Framework. This issue was addressed with improved memory management. (CVE-2018-4196)
- An information disclosure issue existed in device properties. This issue was addressed with improved object management. (CVE-2018-4171)
- An injection issue was addressed with improved input validation. (CVE-2018-4235)
- An input validation issue was addressed with improved input validation. (CVE-2018-4202)
- An issue existed in parsing entitlement plists. This issue was addressed with improved input validation. (CVE-2018-4229)
- An issue existed in the handling of encrypted Mail. This issue was addressed with improved isolation of MIME in Mail. (CVE-2018-4227)
- An issue existed in the handling of S-MIME certificates. This issue was addressed with improved validation of S-MIME certificates. (CVE-2018-4221)
- An out-of-bounds read issue existed that led to the disclosure of kernel memory. This was addressed with improved input validation. (CVE-2018-4253)
- An out-of-bounds read was addressed with improved input validation. (CVE-2018-4222)
- A permissions issue existed in Magnifier. This was addressed with additional permission checks. (CVE-2018-4239)
- A permissions issue existed in the handling of web browser cookies. This issue was addressed with improved restrictions. (CVE-2018-4232)
- A sandbox issue existed in the handling of microphone access. This issue was addressed with improved handling of microphone access. (CVE-2018-4184)
- A validation issue existed in the handling of phone numbers. This issue was addressed with improved validation of phone numbers. (CVE-2018-4100)
- A validation issue existed in the handling of text. This issue was addressed with improved validation of text. (CVE-2018-4198)
- Credentials were unexpectedly sent when fetching CSS mask images. This was addressed by using a CORS-enabled fetch method. (CVE-2018-4190)
- Processing a maliciously crafted message may lead to a denial of service. This issue was addressed with improved message validation. (CVE-2018-4240, CVE-2018-4250)
- In some circumstances, some operating systems may not expect or properly handle an Intel architecture debug exception after certain instructions. The issue appears to be from an undocumented side effect of the instructions. An attacker might utilize this exception handling to gain access to Ring 0 and access sensitive memory or control operating system processes. (CVE-2018-8897)
- Multiple authorization issues were addressed with improved state management. (CVE-2018-4223, CVE-2018-4224, CVE-2018-4225, CVE-2018-4226)

- Multiple denial of service issues were addressed with improved validation. (CVE-2018-4247, CVE-2018-4249)
- Multiple inconsistent user interface issues were addressed with improved state management. (CVE-2018-4188, CVE-2018-4205)
- Multiple issues existed with Siri permissions. This was addressed with improved permission checking. (CVE-2018-4238, CVE-2018-4244, CVE-2018-4252)
- Multiple memory corruption issues were addressed with improved memory handling. (CVE-2018-4193, CVE-2018-4204, CVE-2018-4234, CVE-2018-4236, CVE-2018-4249)
- Multiple race conditions were addressed with improved locking. (CVE-2018-4192, CVE-2018-4228, CVE-2018-4230)
- Multiple type confusion issues were addressed with improved memory handling. (CVE-2018-4219, CVE-2018-4246)
- Multiple validation issues were addressed with improved input sanitization. (CVE-2018-4141, CVE-2018-4159)
- Issues in php were addressed by updating to php version 7.1.16. (CVE-2018-7584)

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.

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/HT208848
https://support.apple.com/en-us/HT208849
https://support.apple.com/en-us/HT208850
https://support.apple.com/en-us/HT208851
https://support.apple.com/en-us/HT208852
https://support.apple.com/en-us/HT208853
https://support.apple.com/en-us/HT208854

CVE:
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-4100
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-4141
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-4159
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-4171
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-4184
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-4188
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-4190
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-4192
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-4193
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-4196

http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-4198
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-4199
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-4200
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-4201
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-4202
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-4204
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-4205
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-4206
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-4211
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-4214
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-4215
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-4218
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-4219
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-4221
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-4222
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-4223
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-4224
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-4225
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-4226
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-4227
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-4228
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-4229
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-4230
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-4232
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-4233
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-4234
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-4235
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-4236
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-4237
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-4238
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-4239
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-4240
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-4241
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-4242
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-4243
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-4244
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-4246
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-4247
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-4249
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-4250
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-4251
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-4252
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-4253
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-7584
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-8897

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/