TLP: WHITE

MS-ISAC CYBERSECURITY ADVISORY

MS-ISAC ADVISORY NUMBER:
2017-088

DATE(S) ISSUED:
09/21/2017

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

OVERVIEW:
Multiple vulnerabilities have been discovered in watchOS, iOS, tvOS, Xcode, and Safari, the most severe of which could allow for arbitrary code execution. watchOS is the mobile operating system for the Apple Watch and is based on the iOS operating system. iOS is a mobile operating system for mobile devices, including the iPhone, iPad, and iPod touch. tvOS is an operating system for the fourth-generation Apple TV digital media player. Xcode is an integrated development environment containing a suite of software development tools developed by Apple Inc. Safari is a web browser available for OS X and Microsoft Windows.

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 4
- iOS Versions prior to 11
- tvOS Versions prior to 11
- Safari Versions prior to 11
- Xcode Versions prior to 9

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

- An ssh:// URL scheme handling issue was addressed through improved input validation. (CVE-2017-1000117)
- Multiple memory corruption issues were addressed with improved memory handling. (CVE-2017-7076, CVE-2017-7134, CVE-2017-7135, CVE-2017-7136, CVE-2017-7137)

- An input validation issue was addressed through improved input validation. (CVE-2017-9800)
- An inconsistent user interface issue was addressed with improved state management. (CVE-2017-7085, CVE-2017-7106)
- A logic issue existed in the handling of the parent-tab. This issue was addressed with improved state management. (CVE-2017-7089)
- A validation issue existed in AutoDiscover V1. This issue was addressed through requiring TLS. (CVE-2017-7088)
- Multiple denial of service issues were addressed through improved memory handling. (CVE-2017-7072)
- A memory corruption issue was addressed with improved validation. (CVE-2017-7097)
- A denial of service issue was addressed through improved validation. (CVE-2017-7118)
- A permissions issue existed. This issue was addressed with improved permission validation. (CVE-2017-7133)
- Multiple memory corruption issues were addressed with improved memory handling. (CVE-2017-7103, CVE-2017-7105, CVE-2017-7108, CVE-2017-7110, CVE-2017-7112)
- Multiple race conditions were addressed with improved validation. (CVE-2017-7115)
- A validation issue was addressed with improved input sanitization. (CVE-2017-7116)

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/HT208103
https://support.apple.com/en-us/HT208112
https://support.apple.com/en-us/HT208113
https://support.apple.com/en-us/HT208115
https://support.apple.com/en-us/HT208116

CVE:
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-7072
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-7076
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-7085
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-7088
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-7089
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-7097
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-7103
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-7105
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-7106
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-7108

http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-7110
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-7112
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-7115
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-7116
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-7118
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-7133
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-7134
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-7135
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-7136
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-7137
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-9800

24x7 Security Operations Center
Multi-State Information Sharing and Analysis Center (MS-ISAC)
31 Tech Valley Drive
East Greenbush, NY 12061
SOC@cisecurity.org - 1-866-787-4722