



**State of Alaska Cyber Security &
Critical Infrastructure
Cyber Advisory**

October 24, 2016

The following cyber advisory was issued by the State of Alaska and was 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.

ADVISORY NUMBER:

SA2016-160

DATE(S) ISSUED:

10/24/2016

SUBJECT:

Multiple Vulnerabilities in Apple Products Could Allow for Arbitrary Code Execution

OVERVIEW:

Multiple vulnerabilities have been discovered in OS X, Safari, watchOS, tvOS, and iOS. OS X is an operating system for Apple computers. Apple Safari is a web browser available for OS X and Microsoft Windows. watchOS is the mobile operating system of the Apple Watch. tvOS is an operating system for Apple TV digital media player. Apple iOS is an operating system for iPhone, iPod touch, and iPad. These vulnerabilities can be exploited if a user visits, or is redirected to, a specially crafted webpage or opens a specially crafted file, including an email attachment.

Successful exploitation of the most severe of these vulnerabilities could result in an attacker gaining the same privileges as the logged on user, arbitrary code execution within the context of the application, 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:

- tvOS prior to 10.0.1 for Apple TV (4th generation)
- iOS prior to 10.1 for iPhone 5 and later, iPad 4th generation and later, iPod touch 6th generation and later
- watchOS prior to 3.1 for All Apple Watch models
- OS X prior to 10.12.1 for OS X Yosemite v10.10.5, OS X El Capitan v10.11.6, and macOS Sierra 10.12

- Safari prior to 10.0.1 for OS X Yosemite v10.10.5, OS X El Capitan v10.11.6, and macOS Sierra 10.12

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 OS X, Safari, tvOS, watchOS, and iOS. Successful exploitation of the most severe of these vulnerabilities could lead to arbitrary code execution. Details of all vulnerabilities are as follows:

- A phishing issue existed in the handling of proxy credentials (CVE-2016-7579).
- An access control issue in the Address Book was addressed through improved file-link validation (CVE-2016-4686).
- A memory corruption issue was addressed through improved memory handling (CVE-2016-4673).
- User interface inconsistencies existed in the handling of relayed calls (CVE-2016-4635).
- An out-of-bounds read was addressed through improved bounds checking (CVE-2016-4660).
- A validation issue was addressed through improved input sanitization (CVE-2016-4680).
- An issue existed within the path validation logic for symlinks (CVE-2016-4679).
- A logic issue was addressed through additional restrictions (CVE-2016-4675).
- An access issue was addressed through additional sandbox restrictions on third party applications (CVE-2016-4664).
- An access issue was addressed through additional sandbox restrictions on third party applications (CVE-2016-4665).
- A logging issue existed in the handling of passwords (CVE-2016-4670).
- Multiple input validation issues existed in MIG generated code (CVE-2016-4669).
- Multiple memory corruption issues were addressed through improved memory handling (CVE-2016-4677).
- A memory corruption issue was addressed through improved lock state checking (CVE-2016-4662).
- A null pointer dereference was addressed through improved locking (CVE-2016-4678).
- A memory corruption issue was addressed through improved memory handling (CVE-2016-4667).
- A memory corruption issue was addressed through improved memory handling (CVE-2016-4674).
- A phishing issue existed in the handling of proxy credentials (CVE-2016-7579).
- A memory corruption issue was addressed through improved memory handling (CVE-2016-4673).
- User interface inconsistencies existed in the handling of relayed calls (CVE-2016-4635).
- An out-of-bounds read was addressed through improved bounds checking (CVE-2016-4660).
- An out-of-bounds write was addressed through improved bounds checking (CVE-2016-4671).
- An out-of-bounds read issue existed in the SGI image parsing (CVE-2016-4682).

- An issue existed within the path validation logic for symlinks (CVE-2016-4679).
- A logic issue was addressed through additional restrictions (CVE-2016-4675).
- An issue existed in the parsing of disk images (CVE-2016-4661).
- A memory corruption issue was addressed through improved input validation (CVE-2016-4663).
- A logging issue existed in the handling of passwords (CVE-2016-4670).
- Multiple input validation issues existed in MIG generated code (CVE-2016-4669).
- Multiple memory corruption issues were addressed through improved memory handling (CVE-2016-4666).
- A cross-origin issue existed with location attributes (CVE-2016-4676).
- Multiple memory corruption issues were addressed through improved memory handling (CVE-2016-4677).
- A phishing issue existed in the handling of proxy credentials (CVE-2016-7579).
- A memory corruption issue was addressed through improved memory handling (CVE-2016-4673).
- An out-of-bounds read was addressed through improved bounds checking (CVE-2016-4660).
- A validation issue was addressed through improved input sanitization (CVE-2016-4680).
- An issue existed within the path validation logic for symlinks (CVE-2016-4679).
- A logic issue was addressed through additional restrictions (CVE-2016-4675).
- An access issue was addressed through additional sandbox restrictions on third party applications (CVE-2016-4664).
- An access issue was addressed through additional sandbox restrictions on third party applications (CVE-2016-4665).
- Multiple input validation issues existed in MIG generated code (CVE-2016-4669).
- Multiple memory corruption issues were addressed through improved memory handling (CVE-2016-4677).

Successful exploitation of the most severe of these vulnerabilities could result in an attacker gaining the same privileges as the logged on user, arbitrary code execution within the context of the application, 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 updates provided by Apple to vulnerable systems immediately after appropriate testing.
- Run all software as a non-privileged user 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 un-trusted websites or follow links provided by unknown or un-trusted sources.

REFERENCES:

Apple:

<https://support.apple.com/en-us/HT207269>
<https://support.apple.com/en-us/HT207270>
<https://support.apple.com/en-us/HT207271>
<https://support.apple.com/en-us/HT207272>
<https://support.apple.com/en-us/HT207275>

CVE:

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-4635>
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-4660>
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-4661>
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-4662>
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-4663>
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-4664>
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-4665>
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-4666>
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-4667>
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-4669>
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-4670>
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-4671>
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-4673>
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-4674>
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-4675>
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-4676>
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-4677>
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-4678>
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-4679>
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-4680>
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-4682>
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-4686>
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-7579>