

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

Traffic Light Protocol (TLP): WHITE information may be distributed without restriction, subject to copyright controls.

<http://www.us-cert.gov/tlp/>

DATE(S) ISSUED:

07/19/2016

SUBJECT:

Multiple Vulnerabilities in Apple Products Could Allow For Arbitrary Code Execution

OVERVIEW:

Multiple vulnerabilities have been discovered in iOS, watchOS, tvOS, iTunes, OS X El Capitan, iCloud, AirPort base stations, and Safari, the most severe of which could allow for arbitrary code execution. Apple iOS is an operating system for iPhone, iPod touch, and iPad. watchOS is the mobile operating system of the Apple Watch. tvOS is an operating system for Apple TV digital media player. Apple iTunes is used to play media files on Microsoft Windows and MAC OS X platforms. OS X El Capitan is an operating system for Macintosh computers. Apple iCloud is an online storage service. Apple AirPort base stations are wireless routers and wireless cards. Apple Safari is a web browser available for OS X and Microsoft Windows. Successful exploitation of the most severe of these vulnerabilities could allow an attacker to execute arbitrary code. Depending on the privileges associated with the user, an attacker could 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.

SYSTEM AFFECTED:

- tvOS prior to 9.2.2 for Apple TV (4th generation)
- iOS prior to 9.3.3 for iPhone 4s and later, iPod touch (5th generation) and later, and iPad 2 and later
- watchOS prior to 2.2.2 for Apple Watch Sport, Apple Watch, Apple Watch Edition, and Apple Watch Hermes
- OS X El Capitan prior to v10.11.6 and Security Update 2016-004 for OS X Yosemite v10.10.5 and OS X El Capitan v10.11 and later
- Safari prior to 9.1.2 for OS X Mavericks v10.9.5, OS X Yosemite v10.10.5, and OS X El Capitan v10.11.6
- iTunes prior to 12.4.2 for Windows 7 and later
- AirPort Base Station Firmware Update 7.6.7 and 7.7.7 for AirPort Express, AirPort Extreme, and AirPort Time Capsule base stations with 802.11n; AirPort Extreme and AirPort Time Capsule base stations with 802.11ac
- iCloud for Windows prior to 5.2.1

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:

Apple has released patches for multiple vulnerabilities that have been discovered in Apple products. The most severe of these vulnerabilities could allow for arbitrary code execution. Details of these vulnerabilities are as follows:

- Multiple memory corruption vulnerabilities in the libxml2 component. (CVE-2016-1836, CVE-2016-4447, CVE-2016-4448, CVE-2016-4483, CVE-2016-4614, CVE-2016-4615, CVE-2016-4616, CVE-2016-4619)
- Information disclosure vulnerability while parsing XML in the libxml2 component. (CVE-2016-4449)
- Multiple memory corruption vulnerabilities in the libxslt component. (CVE-2016-1684, CVE-2016-4607, CVE-2016-4608, CVE-2016-4609, CVE-2016-4610, CVE-2016-4612)
- Multiple memory corruption vulnerabilities for WebKit that may lead to arbitrary code execution. (CVE-2016-4586, CVE-2016-4588, CVE-2016-4589, CVE-2016-4622, CVE-2016-4623, CVE-2016-4624)
- Timing issue in the processing of SVG that may disclose image data from another website. (CVE-2016-4583)
- Memory consumption vulnerability in WebKit that may lead to DoS. (CVE-2016-4592)
- Permissions vulnerability in WebKit when handling location variable that may lead to user information disclosure. (CVE-2016-4591)
- User interface spoofing vulnerability in WebKit. (CVE-2016-4590)
- Cross-protocol cross-site scripting (XPSS) vulnerability in Safari WebKit Javascript Bindings. (CVE-2016-4651)
- Cross-site scripting (XSS) vulnerability in WebKit Page Loading that may lead to exfiltration of data cross-origin. (CVE-2016-4585)
- Multiple memory corruption vulnerabilities in WebKit Page Loading that may lead to arbitrary code execution. (CVE-2016-4584)
- Memory corruption vulnerability that may lead to remote code execution for the CoreGraphics component. (CVE-2016-4637)
- Multiple memory corruption issues found in ImageIO that may lead to arbitrary code execution. (CVE-2016-4631)
- Null pointer dereference that can lead to local arbitrary code execution for the IOAcceleratorFamily component. (CVE-2016-4627)
- Null pointer dereference that can lead to local arbitrary code execution for the IOHIDFamily component. (CVE-2016-4626)
- Multiple memory corruption vulnerabilities in the Kernel component that may lead to local arbitrary code execution. (CVE-2016-1863, CVE-2016-1864, CVE-2016-4582)
- Null pointer dereference that can lead to DoS for the Kernel component. (CVE-2016-1865)
- Access vulnerability in privileged API calls that may lead to disclosure of process list. (CVE-2016-4594)
- Memory initialization vulnerability that can lead to process memory disclosure. (CVE-2016-4587)
- Null pointer dereference that can lead to unexpected restart for the iOS Calendar. (CVE-2016-4605)
- User Interface inconsistencies can lead to audio transmission even after termination of call on FaceTime. (CVE-2016-4635)
- Out-of-bounds vulnerability could lead to kernel memory reading for the IOAcceleratorFamily component. (CVE-2016-4628)
- User interface spoofing vulnerability in Safari. (CVE-2016-4604)
- Privacy issue that can lead to local disclosure of private contact information. (CVE-2016-4593)
- Privacy issue that can display video URL outside of private browsing mode. (CVE-2016-4603)
- Memory corruption vulnerability that may lead to remote code execution for AirPort Base Station Firmware. (CVE-2015-7029)
- Vulnerability in apache_mod_php that may lead to arbitrary code execution. (CVE-2016-4650)

- A null pointer vulnerability in Audio that may lead to denial of service. (CVE-2016-4649)
- A memory corruption vulnerability in Audio that may lead to arbitrary code execution with kernel privileges. (CVE-2016-4647)
- A vulnerability in Audio that may lead to a local user determining kernel mode layout. (CVE-2016-4648)
- A vulnerability in Audio that may lead to the disclosure of user information. (CVE-2016-4646)
- An integer overflow existed in bspatch that may lead to unexpected application termination or arbitrary code execution (CVE-2014-9862)
- An information disclosure vulnerability found in CFNetwork. (CVE-2016-4645)
- A local out-of-bounds read issue in CoreGraphics that may lead to disclosure of kernel memory. (CVE-2016-4652)
- A memory corruption issue in Graphics Drivers that may lead to arbitrary code execution. (CVE-2016-4634)
- Multiple memory corruption issues in ImageIO that may lead to arbitrary code execution. (CVE-2016-4629, CVE-2016-4630)
- A memory consumption issue in ImageIO that may lead to remote denial of service. (CVE-2016-4632)
- Multiple memory corruption issues in Intel Graphics Driver that may lead to arbitrary code execution. (CVE-2016-4633)
- A use-after-free vulnerability in IOSurface that may lead to local arbitrary code execution with kernel privileges. (CVE-2016-4625)
- Multiple memory corruption issues in libc++abi that may lead to arbitrary code execution with root privileges. (CVE-2016-4621)
- Multiple memory corruption issues in libexpat that may lead to unexpected application termination or arbitrary code execution. (CVE-2016-0718)
- Multiple vulnerabilities in LibreSSL that may lead to arbitrary code execution. (CVE-2016-2108, CVE-2016-2109)
- A type confusion vulnerability in Login Window that may lead to root privileges. (CVE-2016-4638)
- A memory corruption vulnerability found in Login Window that may lead to arbitrary code execution. (CVE-2016-4640)
- A type confusion vulnerability in Login Window that may lead to arbitrary code execution. (CVE-2016-4641)
- A memory initialization vulnerability in Login Window that may lead to denial of service. (CVE-2016-4639)
- Multiple vulnerabilities found in OpenSSL that may lead to arbitrary code execution. (CVE-2016-2105, CVE-2016-2106, CVE-2016-2107, CVE-2016-2108, CVE-2016-2109, CVE-2016-2176)
- A memory corruption issue found in QuickTime that may lead to arbitrary code execution. (CVE-2016-4601)
- A memory corruption issue found in QuickTime that may lead to unexpected application termination or arbitrary code execution. (CVE-2016-4599)
- Multiple memory corruption issues found in QuickTime that may lead to unexpected application termination or arbitrary code execution. (CVE-2016-4596, CVE-2016-4597, CVE-2016-4600, CVE-2016-4602)
- A memory corruption issue found in QuickTime that may lead to arbitrary code execution. (CVE-2016-4598)
- A vulnerability found in Safari Login AutoFill that may lead to a user's password being visible. (CVE-2016-4595)

Successful exploitation of the most severe of these vulnerabilities could allow an attacker to execute arbitrary code. Depending on the privileges associated with the user, an attacker could install programs, view, change, or delete data; or create new accounts with full user rights.

RECOMMENDATIONS:

The following actions should 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/HT206903>

<https://support.apple.com/en-us/HT206901>

<https://support.apple.com/en-us/HT206900>

<https://support.apple.com/en-us/HT206905>

<https://support.apple.com/en-us/HT206904>

<https://support.apple.com/en-us/HT206902>

<https://support.apple.com/en-us/HT206849>

<https://support.apple.com/en-us/HT206899>

CVE

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-9862>

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-7029>

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-0718>

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-1684>

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-1836>

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-1863>

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-1864>

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-1865>

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-2105>

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-2106>

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-2107>

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-2108>

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-2109>

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-2176>

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-4447>

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-4448>

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-4449>

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-4483>

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-4582>

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-4583>

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-4584>

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-4585>

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-4586>

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-4587>

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-4588>

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-4589>

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-4590>

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-4591>

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-4592>

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-4593>

TLP: WHITE

Traffic Light Protocol (TLP): WHITE information may be distributed without restriction, subject to copyright controls.

<http://www.us-cert.gov/tlp/>