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:
10/01/2015

SUBJECT:
Multiple Vulnerabilities in Apple Products Could Allow Remote Code Execution

OVERVIEW:
Multiple vulnerabilities have been discovered in Apple Safari, Apple OS X and Apple iOS that could lead to remote code execution. Apple Safari is a web browser usable by many modern operating systems. Apple OS X is an operating system designed to run on Apple Mac Computers. 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 could result in an attacker gaining the same privileges as the logged on user, remote code execution within the context of the application, and the ability to bypass the security system. Failed attacks may still cause a Denial of Service condition within the targeted delivery method. 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.

SYSTEM AFFECTED:
- Apple iOS prior to 9.0.2
- Apple OS X prior to 10.11
- Apple Safari prior to 9

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: High

TECHNICAL SUMMARY:
Multiple vulnerabilities have been discovered in Apple Safari, Apple OS X and Apple iOS that could lead to remote code execution. Details of these vulnerabilities are as follows:

- Multiple vulnerabilities affect the 'Kernel' component, which could allow an attacker to execute arbitrary code. (CVE-2015-5868, CVE-2015-5896, CVE-2015-5903)
- Multiple vulnerabilities in PHP versions prior to 5.5.27 could lead to remote code execution (CVE-2014-9425, CVE-2014-9427, CVE-2014-9652, CVE-2014-9705, CVE-2014-9709, CVE-2015-0231, CVE-2015-0232, CVE-2015-0235, CVE-2015-0273, CVE-2015-1351, CVE-2015-1352, CVE-2015-2301, CVE-2015-2305, CVE-2015-2331, CVE-2015-2348, CVE-2015-2783, CVE-2015-2787, CVE-2015-3329, CVE-2015-3330)
- A memory-corruption vulnerability affects the 'CoreText' component when handling specially-crafted font files. An attacker can exploit this issue to execute arbitrary code. (CVE-2015-5874)
- A memory-corruption vulnerability affects the ‘Dev Tools’ component. An attacker can exploit this issue to execute arbitrary code. (CVE-2015-5876)
- A memory-corruption vulnerability affects the ‘Disk Images’ component. An attacker can exploit this issue to execute arbitrary code. (CVE-2015-5847)
- A memory-corruption vulnerability affects the ‘libc’ component. An attacker can exploit this issue to execute arbitrary code. (CVE-2014-8611)
- A memory-corruption vulnerability affects the ‘libpthread’ component. An attacker can exploit this issue to execute arbitrary code. (CVE-2015-5899)
- A memory-corruption vulnerability affects the ‘IOHIDFamily’ component. An attacker can exploit this issue to execute arbitrary code. (CVE-2015-5867)
- Memory-corruption vulnerabilities affect the ‘JavaScriptCore’ component. An attacker can exploit these issues to execute arbitrary code. (CVE-2015-5791, CVE-2015-5793, CVE-2015-5814, CVE-2015-5816, CVE-2015-5822, CVE-2015-5823)
- Memory-corruption vulnerabilities affect the ‘tidy’ component. An attacker can exploit these issues to execute arbitrary code. (CVE-2015-5522, CVE-2015-5523)
- Webkit is prone multiple memory-corruption vulnerabilities, which could allow for arbitrary code execution. (CVE-2015-5789, CVE-2015-5790, CVE-2015-5792, CVE-2015-5794, CVE-2015-5795, CVE-2015-5796, CVE-2015-5797, CVE-2015-5799, CVE-2015-5800, CVE-2015-5801, CVE-2015-5802, CVE-2015-5803, CVE-2015-5804, CVE-2015-5805, CVE-2015-5806, CVE-2015-5807, CVE-2015-5809, CVE-2015-5810, CVE-2015-5811, CVE-2015-5812, CVE-2015-5813, CVE-2015-5817, CVE-2015-5818, CVE-2015-5819, CVE-2015-5821, CVE-2015-5798, CVE-2015-5808, CVE-2015-5815)
- Malicious audio playback may cause unexpected app termination. (CVE-2015-5862)
- User-activity can be tracked by attacker in privileged network position. (CVE-2015-5885)
- Unintended cookie creation for websites. (CVE-2015-3801)
- Client reconnaissance of other hosts using malicious ftp servers. (CVE-2015-5912)
- Bypass of HTTP Strict Transport Security (HSTS) with a maliciously crafted URL to leak sensitive data. (CVE-2015-5858)
- User-tracking safari private browsing mode with a malicious website. (CVE-2015-5860)
- Assigning malicious cookies for a website by malicious websites. (CVE-2015-5841)
- Interception of SSL/TLS connections by attacker from privileged network position. (CVE-2015-5824)
- Bypass of dyld code signing. (CVE-2015-5839)
- Access of player’s email address by malicious Game Center application. (CVE-2015-5855)
- Memory reading by local attacker. (CVE-2015-5863)
- Stack cookie values controlled by attacker. (CVE-2013-3951)
- Modification of other processes by a local process without entitlement checks. (CVE-2015-5882)

- Ability to launch DoS attacks to TCP connections without sequence number. (CVE-2015-5879)
- Disabling of IPv6 routing by attacker in local LAN segment. (CVE-2015-5869)
- Determination of kernel memory layout by local user. (CVE-2015-5842)
- Observation of unprotected multipeer data by local attacker. (CVE-2015-5851)
- Determination of kernel memory layout by malicious application. (CVE-2015-5831)
- OpenSSL vulnerabilities. (CVE-2015-0286, CVE-2015-0287)
- Unexpected application termination by malicious data processing. (CVE-2015-5840)
- Access to Safari bookmarks on locked iOS device without use of passcode. (CVE-2015-5903)
- User-interface spoofing from malicious website. (CVE-2015-5764, CVE-2015-5765, CVE-2015-5767)
- User-tracking with client certificates by malicious websites. (CVE-2015-1129)
- Object references leak in WebKit. (CVE-2015-5827)
- Unintended dialing by visiting malicious website. (CVE-2015-5820)
- Cross-origin data exfiltration vulnerability. (CVE-2015-5826)
- Leakage of browsing history, mouse movements, and network activity by malicious website. (CVE-2015-5825)
- Disclosure of image data from another site when visiting malicious website. (CVE-2015-5788)
- Arbitrary code execution when opening a media file. (CVE-2010-3190)
- The local communication between Safari extensions and companion apps could be compromise by another native app. A validated extension could be replaced on disk without prompting the user (CVE-2015-5780)
- The Safari plugins may send an HTTP request without knowing the request was redirected which could lead to unauthorized requests(CVE-2015-5828)
- A local arbitrary code injection vulnerability exists in Address Book Framework's handling of environmental variable (CVE-2015-5897)
- An information leakage vulnerability exists in the way Air Scan processed eSCL packets (CVE-2015-5853)
- An information disclosure vulnerability exists with access control lists used for iCloud keychain item (CVE-2015-5836)
- An issue existed that allowed some users to send events to other users (CVE-2015-5849)
- Multiple vulnerabilities in Bash exists because of improper parsing of function definitions in the values of environmental variables which could allow for arbitrary code execution (CVE-2014-6277, CVE-2014-7186, CVE-2014-7187)
- An attacker could prevent the system from booting by using a malicious application with addresses that existed in the protected range register (CVE-2015-5900)
- A malicious Apple Ethernet Thunderbolt adapter could allow an attacker to perform firmware flashing (CVE-2015-5914)
- The "Secure empty trashcan" feature might not securely delete files which could lead to information disclosure (CVE-2015-5901)
- A malicious attacker may be able to play Kerberos credentials to the SMB server (CVE-2015-5913)
- Multiple vulnerabilities in ICU could lead to arbitrary code via especially crafted text (CVE-2014-8146, CVE-2014-8147, CVE-2015-5922)
- A local privilege escalation vulnerability exists in the Install private framework (CVE-2015-5888)

- A local user may execute arbitrary code with system privilege by leveraging the Intel Graphics Driver (CVE-2015-5830, CVE-2015-5877)
- A local attacker may be able to determine the kernel memory layout due to an issue that exists in the IOAudioFamily (CVE-2015-5864)
- A local attacker may be able to execute arbitrary code with kernel privilege due to multiple vulnerabilities that exist in IOGraphics (CVE-2015-5871, CVE-2015-5872, CVE-2015-5873, CVE-2015-5890)
- Multiple memory corruption vulnerabilities exists in IOHIDFamily which could lead to a malicious application executing arbitrary code with system privilege (CVE-2015-5866, CVE-2015-5867)
- A local user may be able to determine kernel memory layout due an issue that exists in the debugging interfaces (CVE-2015-5870)
- A local user maybe able to cause a denial of service to the system due to issues that exist in debugging functionality (CVE-2015-5902)
- Due to a vulnerability that exist in Launchpad a large amount of SSH connections could cause denial of service (CVE-2015-5881)
- An issue existed with the screen lock not engaging after the specified time period (CVE-2015-5833)
- A remote denial of service vulnerability exists in the glob-processing of tnftpd (CVE-2015-5917)
- An attacker in a privileged network position may be able to intercept attachments of s/MIME-encrypted e-mail sent via Mail Drop (CVE-2015-5884)
- A local attacker may be able to access sensitive user information due to a vulnerability that exists when parsing links in the Notes application (CVE-2015-5878)
- A cross site scripting vulnerability in parsing text in the Notes application can lead to information disclosure (CVE-2015-5875)
- Multiple vulnerabilities in OpenSSh were fixed by upgrading the version of OpenSSh used (CVE-2014-2532)
- Multiple vulnerabilities exist in procmail which were fixed by upgrading the version of procmail used (CVE-2014-3618)
- A local user may be able to execute arbitrary code with root privilege due to a vulnerability that exists in the rsh binary (CVE-2015-5889)
- Multiple vulnerabilities that existed with Ruby was fixed by updating the version of Ruby used (CVE-2014-8080, CVE-2014-8090, CVE-2015-1855)
- A state management vulnerability existed in the way keychain lock status was tracked, which could incorrectly display the status of the keychain (CVE-2015-5915)
- A vulnerability with the kSecRevocationRequirePositiveResponse flag could allow a trust evaluation configured to require revocation checking may succeed even if revocation fails (CVE-2015-5894)
- A remote server may prompt for a certificate before identifying itself which could allow information disclosure (CVE-2015-5887)
- A local arbitrary code execution vulnerability exists due to memory corruption issues in the kernel (CVE-2015-5891)
- A local information disclosure vulnerability exists in the SMBClient (CVE-2015-5893)
- Multiple vulnerabilities in SQLite were fixed by updating the version of SQLite used (CVE-2015-3414, CVE-2015-3415, CVE-2015-3416)
- A local attacker can place phone calls without knowledge of the user when using continuity (CVE-2015-3785)

- A maliciously crafted text could mislead users in Terminal due to errors in the way Terminal handled bidirectional override characters (CVE-2015-5883)
- A person with physical access to an iOS device may be able to access photos and contacts from the lock screen leading to information disclosure (CVE-2015-5923)

Successful exploitation could result in an attacker gaining the same privileges as the logged on user, remote code execution within the context of the application, and the ability to bypass the security systems. Failed attacks may still cause a Denial of Service condition within the targeted delivery method. 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:
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 (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 un-trusted websites or follow links provided by unknown or un-trusted sources.

REFERENCES:

Apple:
https://support.apple.com/en-us/HT205267
https://support.apple.com/en-us/HT205284
https://support.apple.com/en-us/HT205265

SecurityFocus:
http://www.securityfocus.com/advisories/36285
http://www.securityfocus.com/advisories/36284

CVE:
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-3951
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-8146
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-8611
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-0231
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-0232
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-0235
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-0273
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-0286
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-0287
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-1129
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-1351
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-1352
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-1855
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-2301
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-2305
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-2331
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-2348

http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-2532
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-2783
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-2787
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-3329
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-3330
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-3414
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-3415
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-3416
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-3618
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-3785
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-3801
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-5522
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-5523
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-5764
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-5765
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-5767
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-5780
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-5788
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-5789
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-5790
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-5791
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-5792
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-5793
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-5794
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-5795
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-5796
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-5797
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-5798
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-5799
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-5800
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-5801
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-5802
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-5803
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-5804
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-5805
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-5806
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-5807
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-5808
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-5809
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-5810
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-5811
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-5812
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-5813
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-5814
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-5815
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-5816
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-5817
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-5818
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-5819
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-5820
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-5821

http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-5822
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-5823
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-5824
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-5825
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-5826
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-5827
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-5828
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-5830
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-5831
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-5833
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-5836
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-5839
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-5840
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-5841
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-5842
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-5844
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-5847
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-5849
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-5851
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-5855
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-5858
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-5860
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-5862
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-5863
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-5864
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-5866
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-5867
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-5867
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-5868
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-5869
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-5870
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-5871
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-5872
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-5873
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-5874
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-5875
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-5876
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-5877
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-5878
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-5879
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-5881
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-5882
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-5883
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-5884
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-5885
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-5887
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-5888
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-5889
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-5890
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-5891
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-5893

http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-5894
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-5896
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-5897
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-5899
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-5900
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-5901
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-5902
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-5903
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-5912
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-5913
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-5914
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-5915
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-5917
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-5922
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-5923
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-6277
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-7186
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-7187
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-8080
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-8090
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-8146
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-8147
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-9425
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-9427
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-9652
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-9705
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-9709

TLP: WHITE
Traffic Light Protocol (TLP): WHITE information may be distributed without restriction, subject to copyright controls.
http://www.us-cert.gov/tlp/