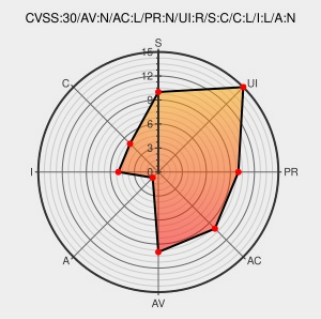
# CVE-2016-4651

Published on: 07/21/2016 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:26:58 PM UTC

## CVE-2016-4651

Source: Mitre | Source: NIST | CVE.ORG | Print: PDF




Certain versions of Iphone Os from Apple contain the following vulnerability:

Cross-site scripting (XSS) vulnerability in the WebKit JavaScript bindings in Apple iOS before 9.3.3 and Safari before 9.1.2 allows remote attackers to inject arbitrary web script or HTML via a crafted HTTP/0.9 response, related to a "cross-protocol cross-site scripting (XPXSS)" vulnerability.

CVE-2016-4651 has been assigned by product-security@apple.com to track the vulnerability - currently rated as MEDIUM severity.

### CVSS3 Score: 6.1 - MEDIUM

| Attack Vector | Attack Complexity | Privileges Required | User Interaction |
|---|---|---|---|
| NETWORK | LOW | NONE | REQUIRED |
| **Scope** | **Confidentiality Impact** | **Integrity Impact** | **Availability Impact** |
| CHANGED | LOW | LOW | NONE |

### CVSS2 Score: 4.3 - MEDIUM

| Access Vector | Access Complexity | Authentication |
|---|---|---|
| NETWORK | MEDIUM | NONE |
| **Confidentiality Impact** | **Integrity Impact** | **Availability Impact** |
| NONE | PARTIAL | NONE |

### CVE References

| Description | Tags | Link |
|---|---|---|
| SecurityFocus | www.securityfocus.com text/html | BUGTRAQ 20160825 WebKitGTK+ Security Advisory WSA-2016-0005 |
| Apple Safari Multiple Bugs Let Remote Users Obtain | www.securitytracker.com | SECTRACK 1036343 |

| | | |
|---|---|---|
| Potentially Sensitive Information, Deny Service, Execute Arbitrary Code, and Spoof User Interface Elements - SecurityTracker | text/html | |
| About the security content of Safari 9.1.2 - Apple Support | Vendor Advisory<br>support.apple.com<br>text/html | CONFIRM support.apple.com/HT206900 |
| About the security content of iOS 9.3.3 - Apple Support | Vendor Advisory<br>support.apple.com<br>text/html | CONFIRM support.apple.com/HT206902 |
| Malformed Request | cve.report (archive)<br>text/html | BID 91835 |
| APPLE-SA-2016-07-18-2 iOS 9.3.3 | Mailing List<br>Vendor Advisory<br>lists.apple.com<br>text/html | APPLE APPLE-SA-2016-07-18-2 |
| APPLE-SA-2016-07-18-5 Safari 9.1.2 | Mailing List<br>Vendor Advisory<br>lists.apple.com<br>text/html | APPLE APPLE-SA-2016-07-18-5 |
| WebKitGTK+ SOP Bypass / Information Disclosure ≈ Packet Storm | packetstormsecurity.com<br>text/html | MISC packetstormsecurity.com/files/138502/WebKitGTK-SOP-Bypass-Information-Disclosure.html |



There are currently no QIDs associated with this CVE

## Known Affected Configurations (CPE V2.3)

| Type | Vendor | Product | Version | Update | Edition | Language |
|---|---|---|---|---|---|---|
| Operating System | Apple | Iphone Os | All | All | All | All |
| Application | Apple | Safari | All | All | All | All |

cpe:2.3:o:apple:iphone_os:*:*:*:*:*:*:*:*:

cpe:2.3:a:apple:safari:*:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→

site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE, CWE, and OVAL are registred trademarks of The MITRE Corporation and the authoritative source of CVE content is MITRE's CVE web site. This site includes MITRE data granted under the following license.

**CVE.report and Source URL Uptime Status status.cve.report**