

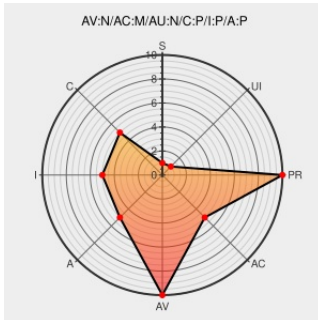


CVE-2015-7014

Published on: 10/23/2015 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:26:12 PM UTC

CVE-2015-7014

[Source: Mitre](#)[Source: NIST](#)[CVE.ORG](#)[Print: PDF](#) 

Certain versions of [Iphone Os](#) from [Apple](#) contain the following vulnerability:

WebKit, as used in Apple iOS before 9.1, Safari before 9.0.1, and iTunes before 12.3.1, allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption and application crash) via a crafted web site, a different vulnerability than other WebKit CVEs listed in APPLE-SA-2015-10-21-1, APPLE-SA-2015-10-21-3, and

APPLE-SA-2015-10-21-5.

CVE-2015-7014 has been assigned by product-security@apple.com to track the vulnerability

CVSS2 Score: **6.8 - MEDIUM**

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

CVE References

Description	Tags	Link
APPLE-SA-2015-10-21-3 Safari 9.0.1	Vendor Advisory lists.apple.com text/html	APPLE APPLE-SA-2015-10-21-3
About the security content of iOS 9.1 - Apple Support	Vendor Advisory support.apple.com text/html	CONFIRM support.apple.com/HT205370
APPLE-SA-2015-10-21-5 iTunes 12.3.1	Patch Vendor Advisory lists.apple.com text/html	APPLE APPLE-SA-2015-10-21-5
WebKit Multiple Unspecified Memory Corruption Vulnerabilities	cve.report (archive)	BID 77267

Apple OS X Multiple Unchecked Memory Corruption Vulnerabilities	CVEreport (archive) text/html	CVE-2016-0761
About the security content of Safari 9.0.1 - Apple Support	Vendor Advisory support.apple.com text/html	CONFIRM support.apple.com/HT205377
openSUSE-SU-2016:0761-1: moderate: Security update for webkit2gtk3	lists.opensuse.org text/html	SUSE openSUSE-SU-2016:0761
Apple OS X Multiple Flaws Let Remote Users Execute Arbitrary Code and Let Apps Gain Elevated Privileges - SecurityTracker	www.securitytracker.com text/html	SECTrack 1033929
About the security content of iTunes 12.3.1 - Apple Support	Vendor Advisory support.apple.com text/html	CONFIRM support.apple.com/HT205372
APPLE-SA-2015-10-21-1 iOS 9.1	Vendor Advisory lists.apple.com text/html	APPLE APPLE-SA-2015-10-21-1

By selecting these links, you may be leaving CVEreport webspace. We have provided these links to other websites because they may have information that would be of interest to you. No inferences should be drawn on account of other sites being referenced, or not, from this page. There may be other websites that are more appropriate for your purpose. CVEreport does not necessarily endorse the views expressed, or concur with the facts presented on these sites. Further, CVEreport does not endorse any commercial products that may be mentioned on these sites. Please address comments about any linked pages to comment@cve.report.

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	Itunes	All	All	All	All
Application	Apple	Safari	All	All	All	All
cpe:2.3:o:apple:iphone_os:*****:*						
cpe:2.3:a:apple:itunes:*****:*						
cpe:2.3:a:apple:safari:*****:*						

No vendor comments have been submitted for this CVE

[← Previous ID](#)

[Next ID →](#)

© CVE.report 2023 |

Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, completeness or usefulness of any information, opinion, advice or other content. EACH USER WILL BE SOLELY RESPONSIBLE FOR ANY consequences of his or her direct or indirect use of this web site. ALL WARRANTIES OF ANY KIND ARE EXPRESSLY DISCLAIMED. This site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE, CWE, and OVAL are registered 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](#).

