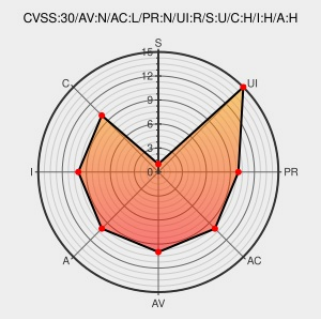
CVE-2016-4622

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

Last Modified on: 03/23/2021 11:26:57 PM UTC

CVE-2016-4622

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



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

WebKit in Apple iOS before 9.3.3, Safari before 9.1.2, and tvOS before 9.2.2 allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted web site, a different vulnerability than CVE-2016-4589, CVE-2016-4623, and CVE-2016-4624.

CVE-2016-4622 has been assigned by product-security@apple.com to track the vulnerability - currently rated as HIGH severity.

CVSS3 Score: 8.8 - HIGH

Attack Vector	Attack Complexity	Privileges Required	User Interaction
NETWORK	LOW	NONE	REQUIRED
Scope	**Confidentiality Impact**	**Integrity Impact**	**Availability Impact**
UNCHANGED	HIGH	HIGH	HIGH

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
SecurityFocus	Third Party Advisory VDB Entry www.securityfocus.com	BUGTRAQ 20160825 WebKitGTK+ Security Advisory WSA-2016-0005

	text/html	
No Description Provided	Third Party Advisory VDB Entry cve.report (archive) text/html	BID 91830
Apple Safari Multiple Bugs Let Remote Users Obtain Potentially Sensitive Information, Deny Service, Execute Arbitrary Code, and Spoof User Interface Elements - SecurityTracker	Third Party Advisory VDB Entry www.securitytracker.com text/html	SECTRACK 1036343
About the security content of Safari 9.1.2 - Apple Support	Vendor Advisory support.apple.com text/html	CONFIRM support.apple.com/HT206900
Zero Day Initiative	Third Party Advisory VDB Entry www.zerodayinitiative.com text/html	MISC www.zerodayinitiative.com/advisories/ZDI-16-486
About the security content of iOS 9.3.3 - Apple Support	Vendor Advisory support.apple.com text/html	CONFIRM support.apple.com/HT206902
APPLE-SA-2016-07-18-4 tvOS 9.2.2	Mailing List Vendor Advisory lists.apple.com text/html	APPLE APPLE-SA-2016-07-18-4
APPLE-SA-2016-07-18-2 iOS 9.3.3	Mailing List Vendor Advisory lists.apple.com text/html	APPLE APPLE-SA-2016-07-18-2
About the security content of tvOS 9.2.2 - Apple Support	Vendor Advisory support.apple.com text/html	CONFIRM support.apple.com/HT206905
Zero Day Initiative	Third Party Advisory VDB Entry www.zerodayinitiative.com text/html	MISC www.zerodayinitiative.com/advisories/ZDI-16-485
APPLE-SA-2016-07-18-5 Safari 9.1.2	Mailing List Vendor Advisory lists.apple.com text/html	APPLE APPLE-SA-2016-07-18-5
WebKitGTK+ SOP Bypass / Information Disclosure ≈ Packet Storm	Third Party Advisory VDB Entry packetstormsecurity.com text/html	MISC packetstormsecurity.com/files/138502/WebKitGTK-SOP-Bypass-Information-Disclosure.html

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

Exploit/POC from Github

My journey through WebKit CVE-2016-4622 Exploitation process

Known Affected Configurations (CPE V2.3)

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

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

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

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

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

cpe:2.3:o:apple:tvos:*:*:*:*:*:*:*:*:

cpe:2.3:o:apple:tvos:*:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

Social Mentions

Source	Title	Posted (UTC)
/r/ExploitDev	What are some instructive non-JIT JavaScript engine bugs?	2020-09-17 00:40:00
/r/AskNetsec	What are some instructive non-JIT JavaScript engine bugs?	2020-09-17 00:35:59

← 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 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