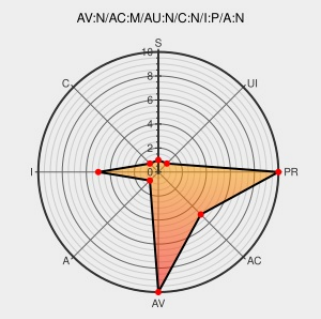
CVE-2015-5828

Published on: 10/08/2015 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:26:14 PM UTC

CVE-2015-5828

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



Certain versions of Safari from Apple contain the following vulnerability:

The API in the WebKit Plug-ins component in Apple Safari before 9 does not provide notification of an HTTP Redirection (aka 3xx) status code to a plugin, which allows remote attackers to bypass intended request restrictions via a crafted web site.

CVE-2015-5828 has been assigned by product-security@apple.com to track the vulnerability

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
About the security content of Safari 9 - Apple Support	Vendor Advisory, support.apple.com, text/html	CONFIRM support.apple.com/HT205265
openSUSE-SU-2016:0761-1: moderate: Security update for webkit2gtk3	Third Party Advisory, lists.opensuse.org, text/html	SUSE openSUSE-SU-2016:0761
APPLE-SA-2015-09-30-2 Safari 9	Vendor Advisory, lists.apple.com, text/html	APPLE APPLE-SA-2015-09-30-2
Apple Safari Extensions and Plug-ins Flaws Let Remote Users Replace Extensions and Redirect Plugin Requests - SecurityTracker	Third Party Advisory, VDB Entry, www.securitytracker.com, text/html	SECTRACK 1033688

Apple Safari WebKit Plug-ins CVE-2015-5828 Security Bypass Vulnerability

Third Party Advisory
VDB Entry
cve.report (archive)
text/html

BID 79707

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Apple	Safari	All	All	All	All
Operating System	Opensuse	Leap	42.1	All	All	All
Operating System	Opensuse	Leap	42.1	All	All	All

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

cpe:2.3:o:opensuse:leap:42.1:*:*:*:*:*:*:*:

cpe:2.3:o:opensuse:leap:42.1:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→