

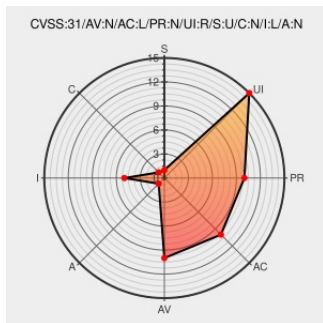


CVE-2020-9945

Published on: 12/08/2020 12:00:00 AM UTC

Last Modified on: 06/02/2022 06:56:00 PM UTC

CVE-2020-9945

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

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

A spoofing issue existed in the handling of URLs. This issue was addressed with improved input validation. This issue is fixed in macOS Big Sur 11.0.1, Safari 14.0.1. Visiting a malicious website may lead to address bar spoofing.

CVE-2020-9945 has been assigned by product-security@apple.com to track the vulnerability - currently rated as **MEDIUM** severity.

Affected Vendor/Software: **Apple** - macOS version < 11.0

Affected Vendor/Software: **Apple** - macOS version < 14.0

CVSS3 Score: **4.3 - MEDIUM**

Attack Vector	Attack Complexity	Privileges Required	User Interaction
NETWORK	LOW	NONE	REQUIRED
Scope	Confidentiality Impact	Integrity Impact	Availability Impact
UNCHANGED	NONE	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
Full Disclosure: APPLE-SA-2020-10-14-1 Apple OS X 10.14.6 (High Sierra) to 10.15.7 (Catalina) and macOS 10.15.7 (Catalina) to 11.0.1 (Big Sur) are vulnerable to a spoofing issue in the handling of URLs. This issue was addressed with improved input validation. This issue is fixed in macOS Big Sur 11.0.1, Safari 14.0.1. Visiting a malicious website may lead to address bar spoofing.		Full Disclosure: APPLE-SA-2020-10-14-1

Full Disclosure: APPLE-SA-2020-12-14-4 Additional information for APPLE-SA-2020-11-13-1 macOS Big Sur 11.0.1	seclists.org text/html	 FULLDISC 20201215 APPLE-SA-2020-12-14-4 Additional information for APPLE-SA-2020-11-13-1 macOS Big Sur 11.0.1
About the security content of macOS Big Sur 11.0.1 - Apple Support	Release Notes Vendor Advisory support.apple.com text/html	 MISC support.apple.com/en-us/HT211931
About the security content of Safari 14.0.1 - Apple Support	Release Notes Vendor Advisory support.apple.com text/html	 MISC support.apple.com/en-us/HT211934
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	Mac Os X	All	All	All	All
Operating System	Apple	Mac Os X	All	All	All	All
Application	Apple	Safari	All	All	All	All
Application	Apple	Safari	All	All	All	All
cpe:2.3:o:apple:mac_os_x:*****:						
cpe:2.3:o:apple:mac_os_x:*****:						
cpe:2.3:a:apple:safari:*****:						
cpe:2.3:a:apple:safari:*****:						

No vendor comments have been submitted for this CVE

Social Mentions

Source	Title	Posted (UTC)
 @RemotelyAlerts	Severity: ?? A spoofing issue existed in the handling... CVE-2020-9945 Link for more: alerts.remotelyrmm.com/CVE-2020-9945	2022-06-02 20:31:21

[← Previous ID](#)

[Next ID →](#)

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](#).

CVE.report and Source URL Uptime Status [status.cve.report](#)