



CVE-2021-1801

Published on: 04/02/2021 12:00:00 AM UTC

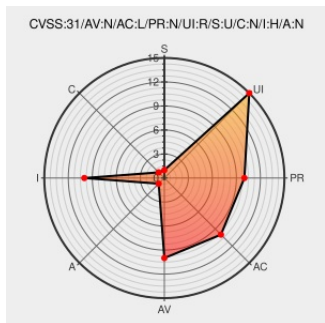
Last Modified on: 06/02/2021 01:20:00 PM UTC

CVE-2021-1801

[Source: Mitre](#)

[Source: Nist](#)

[Print: PDF](#)



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

This issue was addressed with improved iframe sandbox enforcement. This issue is fixed in macOS Big Sur 11.2, Security Update 2021-001 Catalina, Security Update 2021-001 Mojave, watchOS 7.3, tvOS 14.4, iOS 14.4 and iPadOS 14.4. Maliciously crafted web content may violate iframe sandboxing policy.

CVE-2021-1801 has been assigned by product-security@apple.com to track the vulnerability - currently rated as **MEDIUM** severity.

Affected Vendor/Software: **Apple - iOS and iPadOS** version < 14.4

Affected Vendor/Software: **Apple - macOS** version < 11.2

Affected Vendor/Software: **Apple - macOS** version < 7.3

Affected Vendor/Software: **Apple - macOS** version < 14.4

CVSS3 Score: **6.5 - MEDIUM**

Attack Vector	Attack Complexity	Privileges Required	User Interaction
NETWORK	LOW	NONE	REQUIRED
Scope	Confidentiality Impact	Integrity Impact	Availability Impact
UNCHANGED	NONE	HIGH	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
WebkitGTK+: Multiple vulnerabilities (GLSA 202104-03) — Gentoo security	security.gentoo.org text/html	<input type="checkbox"/> GENTOO GLSA-202104-03
About the security content of tvOS 14.4 - Apple Support	support.apple.com text/html	<input type="checkbox"/> MISC support.apple.com/en-us/HT212149
About the security content of macOS Big Sur 11.2, Security Update 2021-001 Catalina, Security Update 2021-001 Mojave - Apple Support	support.apple.com text/html	<input type="checkbox"/> MISC support.apple.com/en-us/HT212147
[SECURITY] Fedora 33 Update: webkit2gtk3-2.32.0-1.fc33 - package-announce - Fedora Mailing-Lists	lists.fedoraproject.org text/html	<input type="checkbox"/> FEDORA FEDORA-2021-864dc37032
About the security content of iOS 14.4 and iPadOS 14.4 - Apple Support	support.apple.com text/html	<input type="checkbox"/> MISC support.apple.com/en-us/HT212146
About the security content of watchOS 7.3 - Apple Support	support.apple.com text/html	<input type="checkbox"/> MISC support.apple.com/en-us/HT212148
[SECURITY] Fedora 32 Update: webkit2gtk3-2.30.6-1.fc32 - package-announce - Fedora Mailing-Lists	lists.fedoraproject.org text/html	<input type="checkbox"/> FEDORA FEDORA-2021-619711d709

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.

Related QID Numbers

- [159499](#) Oracle Enterprise Linux Security Update for GNOME (ELSA-2021-4381)
- [174960](#) SUSE Enterprise Linux Security Update for webkit2gtk3 (SUSE-SU-2021:1430-1)
- [174986](#) SUSE Enterprise Linux Security Update for webkit2gtk3 (SUSE-SU-2021:1499-1)
- [178515](#) Debian Security Update for webkit2gtk (DSA 4877-1)
- [198312](#) Ubuntu Security Notification for Webkit2gtk Vulnerabilities (USN-4894-1)
- [239811](#) Red Hat Update for gnome security (RHSA-2021:4381)
- [281404](#) Fedora Security Update for webkit2gtk3 (FEDORA-2021-619711d709)
- [281405](#) Fedora Security Update for webkit2gtk3 (FEDORA-2021-864dc37032)
- [281406](#) Fedora Security Update for webkit2gtk3 (FEDORA-2021-8070916f7a)
- [501711](#) Alpine Linux Security Update for webkit2gtk
- [710013](#) Gentoo Linux WebkitGTK+ Multiple Vulnerabilities (GLSA 202104-03)
- [750239](#) OpenSUSE Security Update for webkit2gtk3 (openSUSE-SU-2021:0637-1)
- [750655](#) SUSE Enterprise Linux Security Update for webkit2gtk3 (SUSE-SU-2021:1990-1)

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Apple	Ipad Os	All	All	All	All
Operating System	Apple	Iphone Os	All	All	All	All
Operating System	Apple	Macos	All	All	All	All
Operating System	Apple	Tvos	All	All	All	All
Operating System	Apple	Watchos	All	All	All	All
Operating System	Fedoraproject	Fedora	32	All	All	All
Operating System	Fedoraproject	Fedora	33	All	All	All
Application	Webkitgtk	Webkitgtk	All	All	All	All
cpe:2.3:o:apple:ipad_os:*.:.:.:.:.:.:.:						
cpe:2.3:o:apple:iphone_os:*.:.:.:.:.:.:.:						
cpe:2.3:o:apple:macos:*.:.:.:.:.:.:.:						
cpe:2.3:o:apple:tvos:*.:.:.:.:.:.:.:						
cpe:2.3:o:apple:watchos:*.:.:.:.:.:.:.:						
cpe:2.3:o:fedoraproject:fedora:32:*.:.:.:.:.:.:.:						
cpe:2.3:o:fedoraproject:fedora:33:*.:.:.:.:.:.:.:						
cpe:2.3:a:webkitgtk:webkitgtk:*.:.:.:.:.:.:.:						

No vendor comments have been submitted for this CVE

Social Mentions

Source	Title	Posted (UTC)
<input type="checkbox"/> @CVereport	CVE-2021-1801 : This issue was addressed with improved iframe sandbox enforcement. This issue is fixed in macOS Big... twitter.com/i/web/status/1...	2021-04-02 18:51:11

[← Previous ID](#)

[Next ID →](#)

© [CVE.report](#) 2022 |

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](#).

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