

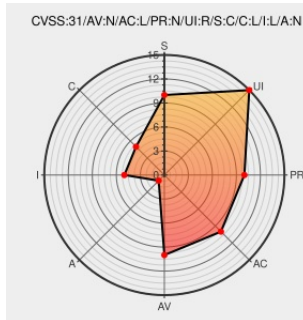


CVE-2019-19916

Published on: 12/20/2019 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:27:54 PM UTC

CVE-2019-19916

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

Certain versions of [Windows 10](#) from [Microsoft](#) contain the following vulnerability:

In Midori Browser 0.5.11 (on Windows 10), Content Security Policy (CSP) is not applied correctly to all parts of multipart content sent with the multipart/x-mixed-replace MIME type. This could result in script running where CSP should have blocked it, allowing for cross-site scripting (XSS) and other attacks when the product renders the content as HTML. Remediating this would also need to consider the polyglot case, e.g., a file that is a valid GIF image and also valid JavaScript.

CVE-2019-19916 has been assigned by [M](#) cve@mitre.org to track the vulnerability - currently rated as **MEDIUM** severity.

CVSS3 Score: **6.1 - MEDIUM**

Attack Vector	Attack Complexity	Privileges Required	User Interaction
NETWORK	LOW	NONE	REQUIRED
Scope	Confidentiality Impact	Integrity Impact	Availability Impact
CHANGED	LOW	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
MIME Confusion Attack on Midori Browser/README.md at master ·	CVE-2019-19916	MISC github.com/41ed1d21x4/MIME

MIME-Confusion-Attack-on-Midori-Browser/README.md at master · V1n1v131r4/MIME-Confusion-Attack-on-Midori-Browser · GitHub	Exploit Third Party Advisory github.com text/html	 MISC github.com/v1n1v131r4/MIME-Confusion-Attack-on-Midori-Browser/blob/master/README.md
Mitigating MIME Confusion Attacks in Firefox - Mozilla Security Blog	Third Party Advisory blog.mozilla.org text/html	 MISC blog.mozilla.org/security/2016/08/26/mitigating-mime-confusion-attacks-in-firefox/
Bypassing CSP using polyglot JPEGs PortSwigger Research	Exploit Third Party Advisory portswigger.net text/html	 MISC portswigger.net/research/bypassing-csp-using-polyglot-jpegs

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	Microsoft	Windows 10	-	All	All	All
Operating System	Microsoft	Windows 10	-	All	All	All
Application	Midori-browser	Midori	0.5.11	All	All	All
Application	Midori-browser	Midori	0.5.11	All	All	All
cpe:2.3:o:microsoft:windows_10:-:*:*:*:*:*:						
cpe:2.3:o:microsoft:windows_10:-:*:*:*:*:*:						
cpe:2.3:a:midori-browser:midori:0.5.11:*:*:*:*:*:						
cpe:2.3:a:midori-browser:midori:0.5.11:*:*:*:*:*:						

No vendor comments have been submitted for this CVE

[← Previous ID](#)

[Next ID →](#)