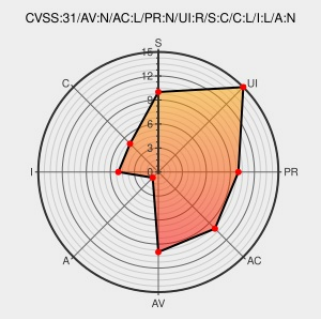
CVE-2019-19916

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 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	Exploit	MISC github.com/V1n1v131r4/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

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→