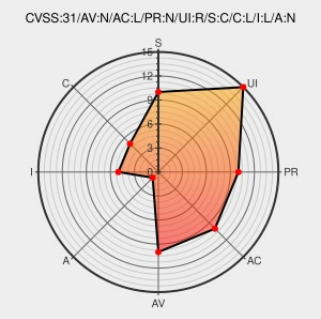
CVE-2021-43532

Published on: Not Yet Published

Last Modified on: 12/10/2021 04:54:00 PM UTC

CVE-2021-43532

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



Certain versions of Firefox from Mozilla contain the following vulnerability:

The 'Copy Image Link' context menu action would copy the final image URL after redirects. By embedding an image that triggered authentication flows - in conjunction with a Content Security Policy that stopped a redirection chain in the middle - the final image URL could be one that contained an authentication token used to takeover a user account. If a website tricked a user into copy and pasting the image link back to the page, the page would be able to steal the authentication tokens. This was fixed by making the action return the original URL, before any redirects. This vulnerability affects Firefox < 94.

CVE-2021-43532 has been assigned by security@mozilla.org to track the vulnerability - currently rated as MEDIUM severity.

Affected Vendor/Software: **Mozilla** - **Firefox** version **< 94**

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: 5.8 - MEDIUM

Access Vector	Access Complexity	Authentication
NETWORK	MEDIUM	NONE
Confidentiality Impact	**Integrity Impact**	**Availability Impact**
PARTIAL	PARTIAL	NONE

CVE References

CVE References

Description	Tags	Link
Access Denied	bugzilla.mozilla.org text/html	MISC bugzilla.mozilla.org/show_bug.cgi?id=1719203
Security Vulnerabilities fixed in Firefox 94 — Mozilla	www.mozilla.org text/html	MISC www.mozilla.org/security/advisories/mfsa2021-48/

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
Application	Mozilla	Firefox	All	All	All	All

cpe:2.3:a:mozilla:firefox:*:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

Social Mentions

Source	Title	Posted (UTC)
@CVEreport	CVE-2021-43532 : The 'Copy Image Link' context menu action would copy the final image URL after redirects. By embed… twitter.com/i/web/status/1…	2021-12-08 22:12:43
/r/netcve	CVE-2021-43532	2021-12-08 22:38:30

← Previous ID

Next ID→

CVE.report and Source URL Uptime Status status.cve.report