

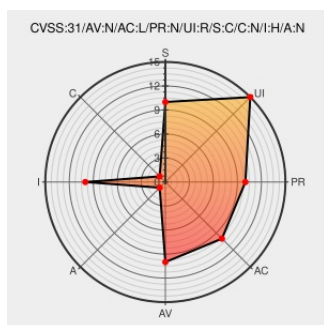


CVE-2021-21354

Published on: 03/08/2021 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:28:58 PM UTC

CVE-2021-21354 - advisory for GHSA-jhgx-wmq8-jc24

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

Certain versions of [Pollbot](#) from [Mozilla](#) contain the following vulnerability:

Pollbot is open source software which "frees its human masters from the toilsome task of polling for the state of things during the Firefox release process." In Pollbot before version 1.4.4 there is an open redirection vulnerability in the path of

"https://pollbot.services.mozilla.com/". An attacker can redirect anyone

to malicious sites. To Reproduce type in this URL:

"https://pollbot.services.mozilla.com//evil.com/". Affected versions will redirect to that website when you inject a payload like "//evil.com/". This is fixed in version 1.4.4.

CVE-2021-21354 has been assigned by security-advisories@github.com to track the vulnerability - currently rated as **MEDIUM** severity.

Affected Vendor/Software: **mozilla** - **PollBot** version < 1.4.4

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

Description	Tags	Link
Access Denied	Issue Tracking Permissions Required Third Party Advisory bugzilla.mozilla.org text/html	bugzilla.mozilla.org/show_bug.cgi?id=1694684
Unvalidated Redirects and Forwards - OWASP Cheat Sheet Series	Third Party Advisory cheatsheetseries.owasp.org text/html	MISC cheatsheetseries.owasp.org/cheatsheets/Unvalidated_Redirects_and_Forwards_Sheet.html
open redirect in [pollbot.services.mozilla.com] · Advisory · mozilla/PollBot · GitHub	Exploit Third Party Advisory github.com text/html	CONFIRM github.com/mozilla/PollBot/security/advisories/GHSA-jhgx-wmq8-jc
Advisory fix 1 by bhearsum · Pull Request #333 · mozilla/PollBot · GitHub	Patch Third Party Advisory github.com text/html	MISC github.com/mozilla/PollBot/pull/333
Release 1.4.4 Release · mozilla/PollBot · GitHub	Third Party Advisory github.com text/html	MISC github.com/mozilla/PollBot/releases/tag/v1.4.4
Remove leading slashes in 404 redirections · mozilla/PollBot@6db74a4 · GitHub	Patch Third Party Advisory github.com text/html	MISC github.com/mozilla/PollBot/commit/6db74a4fcbff258c7cdf51a6ff0724fc1

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	Pollbot	All	All	All	All
Application	Mozilla	Pollbot	All	All	All	All

cpe:2.3:a:mozilla:pollbot:*****:

cpe:2.3:a:mozilla:pollbot:*****:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID →

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](#)