

open redirect in [pollbot.services.mozilla.com]

Low bhearsum published GHSA-jhgx-wmq8-jc24 on Mar 1, 2021

Package	
No package listed	
Affected versions	Patched versions
all	None

Description

(From https://bugzilla.mozilla.org/show_bug.cgi?id=1694684)

Summary:
There is an open redirection vulnerability in the path of:

<https://pollbot.services.mozilla.com/>

Description:
An attacker can redirect anyone to malicious sites.

Steps To Reproduce:
Type in this URL:

<https://pollbot.services.mozilla.com//evil.com/>

As, you can see it redirects to that website when you inject this payload:

`//evil.com/`
evil.com was used as an example but this could be any website note, the `//` is the bypass.

Supporting Material/References:
https://cheatsheetseries.owasp.org/cheatsheets/Unvalidated_Redirects_and_Forwards_Cheat_Sheet.html

Impact

Attackers can serve malicious websites that steal passwords or download ransomware to their victims machine due to a redirect and there are a heap of other attack vectors.

Severity

Low


CVE ID

CVE-2021-21354

Weaknesses

No CWEs

Credits

 eslamXxX156