Improper Restriction of Rendered UI Layers or Frames in yourls/yourls

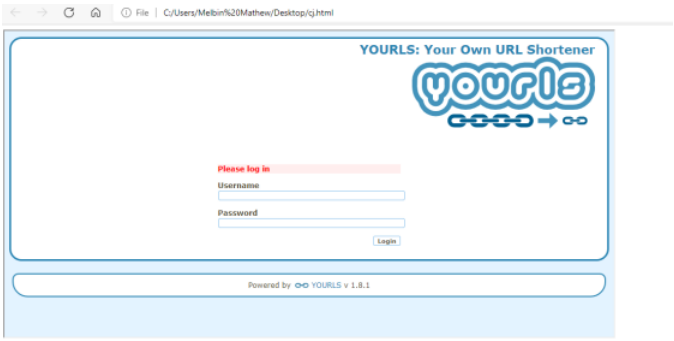
0

Valid Reported on Aug 23rd 2021

✍️ Description

It can be possible to perform a clickjacking attack due to the lack of frame restrictions. The application does not set the response header X-Frame-Options: DENY.

🦹 Proof of Concept



💥 Impact

According to PortSwigger references, it is possible for a page controlled by an attacker to load the website within an iframe. This will enable a clickjacking attack, in which the attacker's page overlays the target application's interface with a different interface provided by the attacker. By inducing victim users to perform actions such as mouse clicks and keystrokes, the attacker can cause them to unwittingly carry out actions within the application that is being targeted. This technique allows the attacker to circumvent defenses against cross-site request forgery and may result in unauthorized actions.

Occurrences

index.php L1

References

- Clickjacking (UI redressing)

CVE
CVE-2021-3734
(Published)

Vulnerability Type
CWE-1021: Improper Restriction of Rendered UI Layers or Frames

Severity
Medium (6.5)

Affected Version
*

Visibility
Public

Status
Fixed

Found by

Melbin Mathew Antony
@melbinkm
amateur

This report was seen 669 times.

We have contacted a member of the yourls team and are waiting to hear back a year ago

A yourls/yourls maintainer a year ago Maintainer

Yeah, indeed. I'd qualify this as low severity but it's also a trivial fix. I'll fix this asap. Thanks for the heads up.

ÒẓĦ a year ago Maintainer

Issue fixed in
https://github.com/YOURLS/YOURLS/commit/0a70acdcfb5fcbc63dbc5750018d608288eba3fe

ÒẓĦ validated this vulnerability a year ago

Melbin Mathew Antony has been awarded the disclosure bounty ✔

The fix bounty is now up for grabs

ÒẓĦ marked this as fixed with commit **0a70ac** a year ago

The fix bounty has been dropped ✖

This vulnerability will not receive a CVE ✖

ÒẓĦ a year ago Maintainer

I clicked on "mark valid" and "confirm fix", I hope this was expected by people using this site.

This said, I'm not sure rewarding disclosure four times the amount of fixing is very virtuous and in the true spirit of open source. Just my 2 cents :)

amammad a year ago

@maintainer you're the real man!!

Jamie Slome a year ago Admin

CVE published! 🎉

Michael Simon a year ago

@maintainer will you be cutting a 1.8.2 build soon?

Sign in to join this conversation