Improper Resolution of Path Equivalence in microweber-dev/whmcs_plugin

2

Valid Reported on Feb 28th 2022

DESCRIPTION

Open redirection vulnerabilities arise when an application incorporates user-controllable data into the target of a redirection in an unsafe way. An attacker can construct a URL within the application that causes a redirection to an arbitrary external domain. This behavior can be leveraged to facilitate phishing attacks against users of the application. The ability to use an authentic application URL, targeting the correct domain and with a valid SSL certificate (if SSL is used), lends credibility to the phishing attack because many users, even if they verify these features, will not notice the subsequent redirection to a different domain.

STEPS TO REPRODUCE:

There is an open redirection vulnerability in the path of = https://microweber.com/get-started?ref=susp#frameurl=
here is " frameurl= " are vulnerable for open redirect
you bypass this vulnerbility using BASE64 encoded mathod
"https://bing.com" encode this url in base64 so its looks like =
aHR0cHM6Ly9iaW5nLmNvbQ==
SO YOU CAN VISIT URL = https://microweber.com/get-started?ref=susp#frameurl=aHR0cHM6Ly9iaW5nLmNvbQ==
YOU CAN SEE THAT URL REDIRECT TO BING.COM

Impact

An http parameter may contain a URL value and could cause the web application to redirect the request to the specified URL. By modifying the URL value to a malicious site, an attacker may successfully launch a phishing scam and steal user credentials. Because the server name in the modified link is identical to the original site, phishing attempts have a more trustworthy appearance.

Occurrences

Occurrences

JS embed.js L64-L74

References

- IBM
- microsoft
- nvd.nist
- mitre1

CVE
CVE-2022-0855
(Published)

Vulnerability Type
CWE-41: Improper Resolution of Path Equivalence

Severity
High (7.4)

Visibility
Public

Status
Fixed

Found by

Piyush shukla
@piyushshukla599
unranked

Fixed by

Peter Ivanov
@peter-mw
maintainer

This report was seen 628 times.

We are processing your report and will contact the microweber-dev/whmc
within 24 hours. 9 months ago

Chat with us

We created a **GitHub Issue** asking the maintainers to create a `SECURITY.md` 9 months ago

Peter Ivanov validated this vulnerability 9 months ago

Piyush shukla has been awarded the disclosure bounty ✔

The fix bounty is now up for grabs

Peter Ivanov marked this as fixed in **0.0.4** with commit **2e7a11** 9 months ago

Peter Ivanov has been awarded the fix bounty ✔

This vulnerability will not receive a CVE ✖

embed.js#L64-L74 has been validated ✔

Piyush shukla 9 months ago — Researcher

hello I'm waiting for CVE ID

Piyush shukla 9 months ago — Researcher

any bounty ?

Jamie Slome 9 months ago — Admin

We can go ahead and publish a CVE if the maintainer is happy to do so. With regards to the bounty, this repository is not deemed popular enough by our pricing model to warrant bounty rewards.

Jamie Slome 9 months ago — Admin

@maintainer - can you please confirm that you are happy for us to assign and publish a CVE?

Peter Ivanov 9 months ago — Maintainer

hi, yes you can assign CVE @admin

Jamie Slome 9 months ago Admin

CVE assigned and published! 🎊

Piyush shukla 9 months ago Researcher

CVE ID ?

Piyush shukla 9 months ago Researcher

Hello Thanks for assigned CVE

I want to know when are the Description and References going to be updated on https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-0855 ?

Jamie Slome 9 months ago Admin

Once this PR has been merged, the details will be made available on MITRE/NVD.

Peter Ivanov 20 days ago Maintainer

Hi, this CVE is not part of Microweber CMS and PR cannot be done.

The error is on the template side and not part of the CMS

❤ Peter Ivanov gave praise 20 days ago

@admin bug if fixed in this repo https://github.com/microweber-dev/whmcs_plugin/blob/master/modules/addons/microweber_addon/order/embed.js#L79-L82

The researcher's credibility has slightly increased as a result of the maintainer's thanks: +1

Pavlos 16 days ago Admin

Hey Peter! Do you want the fix commit SHA or the CVE ratified?

Peter Ivanov 15 days ago Maintainer

Hi, this is the commit https://github.com/microweber-dev/whmcs_plugin/commit/06bf36d43f1334f059677d404b2a94edf94a1095#diff-1cb1f5725f531f6da8a8696c5755be5c43f547d797b7141804bb00cc292f3d1b

Peter Ivanov 15 days ago Maintainer

if you move this report to the repository of https://github.com/microweber-dev/whmcs_plugin/ i will be able to mark it

Sign in to join this conversation