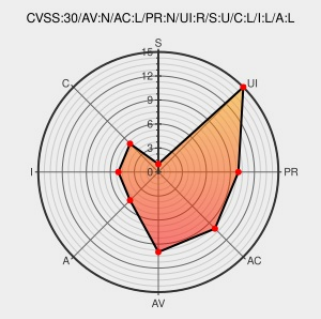
CVE-2022-1439

Published on: Not Yet Published

Last Modified on: 04/29/2022 04:31:00 AM UTC

CVE-2022-1439 - advisory for 86f6a762-0f3d-443d-a676-20f8496907e0

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



Certain versions of Microweber from Microweber contain the following vulnerability:

Reflected XSS on demo.microweber.org/demo/module/ in GitHub repository microweber/microweber prior to 1.2.15. Execute Arbitrary JavaScript as the attacked user. It's the only payload I found working, you might need to press "tab" but there is probably a paylaod that runs without user interaction.

CVE-2022-1439 has been assigned by security@huntr.dev to track the vulnerability - currently rated as MEDIUM severity.

Affected Vendor/Software: **microweber** - **microweber/microweber** version **< 1.2.15**

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: 4.3 - MEDIUM

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

CVE References

Description	Tags	Link
update ·	github.com	MISC

microweber/microweber@ad3928f · GitHub	text/html	github.com/microweber/microweber/commit/ad3928f67b2cd4443f4323d858b
huntr – Security Bounties for any GitHub repository	huntr.dev text/html Inactive Link Not Archived	CONFIRM huntr.dev/bounties/86f6a762-0f3d-443d-a676-20f8496907e0

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	Microweber	Microweber	All	All	All	All

cpe:2.3:a:microweber:microweber:*:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

Social Mentions

Source	Title	Posted (UTC)
@CVEreport	CVE-2022-1439 : Reflected #XSS on demo.microweber.org/demo/module/ in GitHub repository microweber/microweber prior to 1.2.1… twitter.com/i/web/status/1…	2022-04-22 16:32:41
@huntrHacktivity	Cross-site Scripting (XSS) - Reflected in github.com/microweber/mic… (CVE-2022-1439) reported by wfinn - Patch:… twitter.com/i/web/status/1…	2022-04-22 17:07:26
@OpenSourceHacks	(CVE-2022-1439): Cross-site Scripting (XSS) - Reflected in microweber/microweber. huntr.dev/bounties/86f6a… Disclos… twitter.com/i/web/status/1…	2022-04-23 16:26:19
@threatmeter	CVE-2022-1439 | Microweber up to 1.2.14 cross site scripting A vulnerability classified as problematic has been fou… twitter.com/i/web/status/1…	2022-04-24 07:50:25
/r/netcve	CVE-2022-1439	2022-04-22 17:38:24

← Previous ID Next ID→