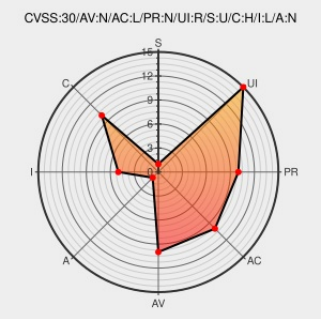
CVE-2022-0926

Published on: Not Yet Published

Last Modified on: 03/18/2022 07:57:00 PM UTC

CVE-2022-0926 - advisory for dc5d1555-0108-4627-b542-93352f35fa17

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



Certain versions of Microweber from Microweber contain the following vulnerability:

File upload filter bypass leading to stored XSS in GitHub repository microweber/microweber prior to 1.2.12.

CVE-2022-0926 has been assigned by security@huntr.dev to track the vulnerability - currently rated as MEDIUM severity.

Affected Vendor/Software: **microweber** - **microweber/microweber** version **< 1.2.12**

CVSS3 Score: 4.8 - MEDIUM

Attack Vector	Attack Complexity	Privileges Required	User Interaction
NETWORK	LOW	HIGH	REQUIRED
Scope	**Confidentiality Impact**	**Integrity Impact**	**Availability Impact**
CHANGED	LOW	LOW	NONE

CVSS2 Score: 3.5 - LOW

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

CVE References

Description	Tags	Link
huntr – Security Bounties for any GitHub repository	huntr.dev text/html Inactive Link Not Archived	CONFIRM huntr.dev/bounties/dc5d1555-0108-4627-b542-93352f35fa17

Update Files.php · microweber/microweber@89200cf · GitHub	github.com text/html	MISC github.com/microweber/microweber/commit/89200cfcc2cfefe5554721e7fa3c

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)
@huntrHacktivity	Cross-site Scripting (XSS) - Stored in github.com/microweber/mic… (CVE-2022-0926) reported by @@rajesh_patil013 - Patc… twitter.com/i/web/status/1…	2022-03-11 10:09:09
@CVEreport	CVE-2022-0926 : File upload filter bypass leading to stored #XSS in GitHub repository microweber/microweber prior t… twitter.com/i/web/status/1…	2022-03-12 10:12:16

← Previous ID

Next ID→