



CVE-2022-2731

Published on: Not Yet Published

Last Modified on: 08/12/2022 02:16:00 PM UTC

CVE-2022-2731 - advisory for 20b8d5c5-0764-4f0b-8ab3-b9f6b857175e

[Source: Mitre](#)

[Source: NIST](#)

[CVE.ORG](#)

[Print: PDF](#)



Certain versions of [Openemr](#) from [Open-emr](#) contain the following vulnerability:

Cross-site Scripting (XSS) - Reflected in GitHub repository [openemr/openemr](#) prior to 7.0.0.1.

CVE-2022-2731 has been assigned by security@huntr.dev to track the vulnerability - currently rated as **MEDIUM** severity.

Affected Vendor/Software: **openemr** - **openemr/openemr** version < 7.0.0.1

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

CVE References

Description	Tags	Link
bug fix e1 · openemr/openemr@285fb23 · GitHub	github.com text/html	MISC github.com/openemr/openemr/commit/285fb234bd27ea4c46a29f2797edda7f38f1c
huntr – Security Bounties for any GitHub repository	huntr.dev text/html Inactive Link Not Archived	CONFIRM huntr.dev/bounties/20b8d5c5-0764-4f0b-8ab3-b9f6b857175e

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	Open-emr	Openemr	All	All	All	All
cpe:2.3:a:open-emr:openemr:*****:*						

No vendor comments have been submitted for this CVE

Social Mentions

Source	Title	Posted (UTC)
 @CVEreport	CVE-2022-2731 : Cross-site Scripting #XSS - Reflected in GitHub repository openemr/openemr prior to 7.0.0.1.... cve.report/CVE-2022-2731	2022-08-09 12:10:45
 @threatmeter	CVE-2022-2731 Cross-site Scripting (XSS) - Reflected in GitHub repository openemr/openemr prior to 7.0.0.1. (CVSS:0... twitter.com/i/web/status/1...	2022-08-09 23:22:23
 @ColorTokensInc	Emerging Vulnerability Found CVE-2022-2731 - Cross-site Scripting (XSS) - Reflected in GitHub repository openemr/op... twitter.com/i/web/status/1...	2022-08-09 23:22:29
 @threatmeter	CVE-2022-2731 Cross-site Scripting (XSS) - Reflected in GitHub repository openemr/openemr prior to 7.0.0.1. (CVSS:0... twitter.com/i/web/status/1...	2022-08-10 07:10:24
 @phpadvisories	CVE-2022-2731 OpenEMR up to 7.0.0.0 cross site scripting zpr.io/ZbdQzZc6BV69 #phpsec	2022-08-10 16:22:53
 @OpenSourceHacks	(CVE-2022-2731): Cross-site Scripting (XSS) - Reflected in openemr/openemr. huntr.dev/bounties/20b8d... Disclosed by... twitter.com/i/web/status/1...	2022-08-12 11:56:47
 /r/netcve	CVE-2022-2731	2022-08-09 12:38:35

[← Previous ID](#)

[Next ID →](#)

© [CVE.report](#) 2023   |

Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, completeness or usefulness of any information, opinion, advice or other content. EACH USER WILL BE SOLELY RESPONSIBLE FOR ANY consequences of his or her direct or indirect use of this web site. ALL WARRANTIES OF ANY KIND ARE EXPRESSLY DISCLAIMED. This site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE, CWE, and OVAL are registered trademarks of [The MITRE Corporation](#) and the authoritative source of CVE content is [MITRE's CVE web site](#). This site includes MITRE data granted under the following [license](#).

CVE.report and Source URL Uptime Status [status.cve.report](#)