

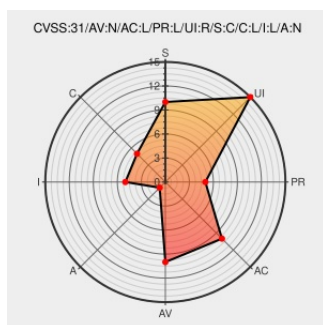


CVE-2021-32852

Published on: Not Yet Published

Last Modified on: 03/06/2023 04:35:00 AM UTC

CVE-2021-32852 - advisory for GHSL-2021-104

[Source: Mitre](#)[Source: NIST](#)[CVE.ORG](#)[Print: PDF](#)

Certain versions of [Countly Server](#) from [Countly](#) contain the following vulnerability:

Countly, a product analytics solution, is vulnerable to cross-site scripting prior to version 21.11 of the community edition. The victim must follow a malicious link or be redirected there from malicious web site. The attacker must have an account or be able to create one. This issue is patched in version 21.11.

CVE-2021-32852 has been assigned by [security-advisories@github.com](#) to track the vulnerability - currently rated as **CRITICAL** severity.

Affected Vendor/Software: [Countly](#) - **countly-server** version < 21.11

CVSS3 Score: **9 - CRITICAL**

Attack Vector	Attack Complexity	Privileges Required	User Interaction
NETWORK	LOW	LOW	REQUIRED
Scope	Confidentiality Impact	Integrity Impact	Availability Impact
CHANGED	HIGH	HIGH	HIGH

CVE References

Description	Tags	Link
GHSL-2021-104: Cross-Site Scripting in countly-server - CVE-2021-32852 GitHub Security Lab	securitylab.github.com text/html	CONFIRM securitylab.github.com/advisories/GHSL-2021-104-c
countly-server/app.js at 6b90bb775e747cabe46fe197c6a6989acc6c3417 · Countly/countly-server · GitHub	github.com text/html	MISC github.com/Countly/countly-server/blob/6b90bb775e747cabe46fe197c6a6989acc6c3417/front
Release v21.11 · Countly/countly-server · GitHub	github.com text/html	MISC github.com/Countly/countly-server/releases/tag/v21.11
countly-server/reset.html at 6b90bb775e747cabe46fe197c6a6989acc6c3417	github.com text/html	MISC github.com/Countly/countly-server/blob/6b90bb775e747cabe46fe197c6a6989acc6c3417/front

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	Count	Countly Server	All	All	All	All
cpe:2.3:a:count:countly_server:*:*:*:community:*:*:						

No vendor comments have been submitted for this CVE

Social Mentions

Source	Title	Posted (UTC)
 @GHSecurityLab	GHSL-2021-104: Cross-Site Scripting (XSS) in countly-server - CVE-2021-32852 github.co/3AM0dOo	2022-02-01 17:30:05
 @CVEreport	CVE-2021-32852 : Countly, a product analytics solution, is vulnerable to cross-site scripting prior to version 21.1... twitter.com/i/web/status/1...	2023-02-20 22:10:00

[← 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](#)