



CVE-2022-32172

Published on: Not Yet Published

Last Modified on: 11/07/2022 08:20:00 PM UTC

CVE-2022-32172 - advisory for <https://www.mend.io/vulnerability-database/>

Source: Mitre

Source: NIST

CVE.ORG

Print: PDF



Certain versions of **Zinc** from **Zinclabs** contain the following vulnerability:

In Zinc, versions v0.1.9 through v0.3.1 are vulnerable to Stored Cross-Site Scripting when using the delete template functionality. When an authenticated user deletes a template with a XSS payload in the name field, the Javascript payload will be executed and allow an attacker to access the user's credentials.

CVE-2022-32172 has been assigned by vulnerabilitylab@whitesourcesoftware.com to track the vulnerability - currently rated as **MEDIUM** severity.

Affected Vendor/Software: **zinc** - **zinc** version **>= v0.1.9**

Affected Vendor/Software: **zinc** - **zinc** version **<= v0.3.1**

CVSS3 Score: **5.4 - MEDIUM**

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

CVE References

Description	Tags	Link
Hotfix/mend vulnerabilities (#521) · zinclabs/zinc@3376c24 · GitHub	github.com text/html	MISC github.com/zinclabs/zinc/commit/3376c248bade163430f9347742428f0a82cd322d
cve-website	www.cve.org text/html	MISC www.cve.org/CVERecord?id=CVE-2022-32172
CVE-2022-32172 Mend Vulnerability Database	www.mend.io text/html	MISC www.mend.io/vulnerability-database/CVE-2022-32172

By providing these links you may be helping CVE-report databases. We have provided these links to other websites because they may have information that

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	Zinlabs	Zinc	All	All	All	All
cpe:2.3:a:zinlabs:zinc:*****:						

Discovery Credit

Mend Vulnerability Research Team (MVR)

Social Mentions

Source	Title	Posted (UTC)
 @CVEreport	CVE-2022-32172 : In Zinc, versions v0.1.9 through v0.3.1 are vulnerable to Stored Cross-Site Scripting when using t... twitter.com/i/web/status/1...	2022-10-06 17:33:57
 @JohnJasonFallow	New vulnerability on the NVD: CVE-2022-32172 ift.tt/IOCLc7E	2022-10-06 20:16:40
 @doogsineerg	New vulnerability on the NVD: CVE-2022-32172 ift.tt/NOKMnIs	2022-10-06 20:33:05
 @workentin	New vulnerability on the NVD: CVE-2022-32172 ift.tt/vk8xAsO	2022-10-06 20:40:18

[← 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](#)