



CVE-2022-34625

Published on: Not Yet Published

Last Modified on: 08/08/2022 07:28:00 PM UTC

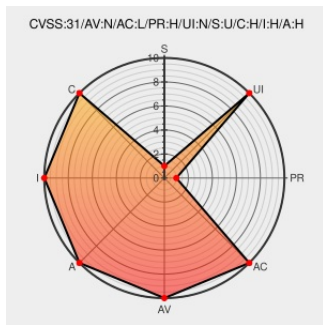
CVE-2022-34625

[Source: Mitre](#)

[Source: NIST](#)

[CVE.ORG](#)

[Print: PDF](#)



Certain versions of [Mealie](#) from [Mealie Project](#) contain the following vulnerability:

Mealie 1.0.0beta3 was discovered to contain a Server-Side Template Injection vulnerability, which allows attackers to execute arbitrary code via a crafted Jinja2 template.

CVE-2022-34625 has been assigned by [M](#) cve@mitre.org to track the vulnerability - currently rated as **HIGH** severity.

CVSS3 Score: **7.2 - HIGH**

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

CVE References

Description	Tags	Link
CWE - CWE-94: Improper Control of Generation of Code ('Code Injection') (4.7)	cwe.mitre.org text/html	cwe.mitre.org/data/definitions/94.html
CWE - CWE-1336: Improper Neutralization of Special Elements Used in a Template Engine (4.6)	cwe.mitre.org text/html	cwe.mitre.org/data/definitions/1336.html
v0.5.6 Bug Fixes - Mealie	docs.mealie.io text/html	docs.mealie.io/changelog/v0.5.6/
CVE-2022-34625 - Server-Side Template Injection to Remote Code Execution (SSTI) to (RCE) in Mealie - A lesson in patience - GainSec	gainsec.com text/html	gainsec.com/2022/08/02/cve-2022-34625-ssti-rce-mealie/
Docker Hub	hub.docker.com text/html	hub.docker.com/r/hkotel/mealie

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	Mealie Project	Mealie	1.0.0	beta3	All	All
<code>cpe:2.3:a:mealie_project:mealie:1.0.0:beta3:*:*:*:*:*:</code>						

No vendor comments have been submitted for this CVE

Social Mentions

Source	Title	Posted (UTC)
 @CVEreport	CVE-2022-34625 : Mealie1.0.0beta3 was discovered to contain a Server-Side Template Injection vulnerability, which a... twitter.com/i/web/status/1...	2022-08-02 16:01:04
 @Robo_Alerts	Potentially Critical CVE Detected! CVE-2022-34625 Mealie1.0.0beta3 was discovered to contain a Server-Side Template... twitter.com/i/web/status/1...	2022-08-02 17:55:59
 @GainSec	CVE-2022-34625 – (SSTI) to (RCE) in Mealie – A lesson in patience Follow @gainsec ? gainsec.com/2022/08/02/cve..... twitter.com/i/web/status/1...	2022-08-04 04:22:18
 /r/netcve	CVE-2022-34625	2022-08-02 16:38:11

[← 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](#)