

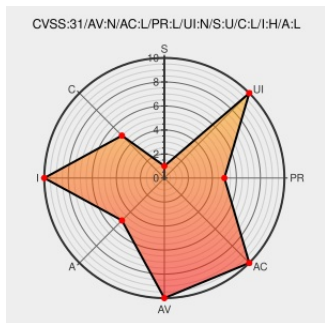


CVE-2022-31041

Published on: Not Yet Published

Last Modified on: 06/23/2022 06:26:00 PM UTC

CVE-2022-31041 - advisory for GHSA-h85r-xv4w-cg8g

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

Certain versions of [Open Forms](#) from [Maykinmedia](#) contain the following vulnerability:

Open Forms is an application for creating and publishing smart forms. Open Forms supports file uploads as one of the form field types. These fields can be configured to allow only certain file extensions to be uploaded by end users (e.g. only PDF / Excel / ...). The input validation of uploaded files is insufficient in versions prior to 1.0.9 and 1.1.1.

Users could alter or strip file extensions to bypass this validation. This results in files being uploaded to the server that are of a different file type than indicated by the file name extension. These files may be downloaded (manually or automatically) by staff and/or other applications for further processing. Malicious files can therefore find their way into internal/trusted networks. Versions 1.0.9 and 1.1.1 contain patches for this issue. As a workaround, an API gateway or intrusion detection solution in front of open-forms may be able to scan for and block malicious content before it reaches the Open Forms application.

CVE-2022-31041 has been assigned by [security-advisories@github.com](#) to track the vulnerability - currently rated as **MEDIUM** severity.

Affected Vendor/Software: [open-formulieren](#) - **open-forms** version < 1.0.9

Affected Vendor/Software: [open-formulieren](#) - **open-forms** version >= 1.1.0-rc0, < 1.1.1

CVSS3 Score: **6.5 - MEDIUM**

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

CVSS2 Score: **4 - MEDIUM**

Access Vector	Access Complexity	Authentication
---------------	-------------------	----------------

Vector	Complexity	
NETWORK	LOW	SINGLE
Confidentiality Impact	Integrity Impact	Availability Impact
NONE	PARTIAL	NONE

CVE References

Description	Tags	Link
Insufficient content-type validation for uploaded files - Advisory · open-formulieren/open-forms · GitHub	github.com text/html	CONFIRM github.com/open-formulieren/open-forms/security/advisories/GHSA-h85r-xv4w-cg8g
Merge pull request from GHSA-h85r-xv4w-cg8g · open-formulieren/open-forms@0978a29 · GitHub	github.com text/html	MISC github.com/open-formulieren/open-forms/commit/0978a29e821a7228c5d46c0527c3e925eb91b071

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	Maykinmedia	Open Forms	All	All	All	All
Application	Maykinmedia	Open Forms	1.1.0	-	All	All
Application	Maykinmedia	Open Forms	1.1.0	rc0	All	All
Application	Maykinmedia	Open Forms	1.1.0	rc1	All	All
cpe:2.3:a:maykinmedia:open_forms:*:*:*:*:*:						
cpe:2.3:a:maykinmedia:open_forms:1.1.0:-:*:*:*:*:						
cpe:2.3:a:maykinmedia:open_forms:1.1.0:rc0:*:*:*:*:						
cpe:2.3:a:maykinmedia:open_forms:1.1.0:rc1:*:*:*:*:						

No vendor comments have been submitted for this CVE

Social Mentions

Source	Title	Posted (UTC)
@CVEreport	CVE-2022-31041 : Open Forms is an application for creating and publishing smart forms. Open Forms supports file upl... twitter.com/i/web/status/1...	2022-06-13 12:39:53
@RemotelyAlerts	Severity: ?? Open Forms is an application for creatin... CVE-2022-31041 Link for more: alerts.remotelyrmm.com/CVE-2022-31041	2022-06-23 19:29:40
/r/netcve	CVE-2022-31041	2022-06-13 13:38:43

© [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](#)