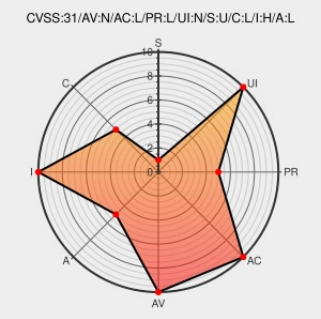
CVE-2022-31041

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

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

← Previous ID

Next ID→