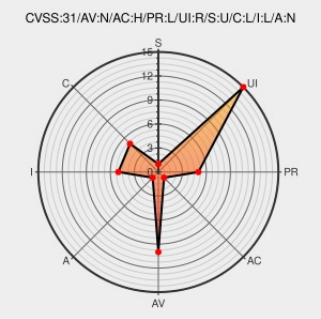
CVE-2020-4061

Published on: 07/02/2020 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:23:22 PM UTC

CVE-2020-4061 - advisory for GHSA-3pc2-fm7p-q2vg

Source: Mitre | Source: NIST | CVE.ORG | Print: PDF



Certain versions of October from Octobercms contain the following vulnerability:

In October from version 1.0.319 and before version 1.0.467, pasting content copied from malicious websites into the Froala richeditor could result in a successful self-XSS attack. This has been fixed in 1.0.467.

CVE-2020-4061 has been assigned by security-advisories@github.com to track the vulnerability - currently rated as MEDIUM severity.

Affected Vendor/Software: **October CMS** - **October** version **>= 1.0.319, < 1.0.467**

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

CVSS2 Score: 3.5 - LOW

Access Vector	Access Complexity	Authentication
NETWORK	MEDIUM	SINGLE
Confidentiality Impact	**Integrity Impact**	**Availability Impact**
NONE	PARTIAL	NONE

CVE References

Description	Tags	Link
The Curious Case of Copy & Paste - on risks of pasting	Exploit Third Party Advisory	MISC research.securitum.com/the-curious-case-of-copy-paste/

arbitrary content in browsers - research.securitum.com	research.securitum.com text/html	
Improve Froala sanitization of pasted content. · octobercms/october@b384954 · GitHub	Patch Third Party Advisory github.com text/html	MISC github.com/octobercms/october/commit/b384954a29b89117e1c0d6035b3ede4f46c
Potential self-XSS when pasting content from malicious websites · Advisory · octobercms/october · GitHub	Third Party Advisory github.com text/html	CONFIRM github.com/octobercms/october/security/advisories/GHSA-3pc2-fm7p-q2vg

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	Octobercms	October	All	All	All	All
Application	Octobercms	October	All	All	All	All

cpe:2.3:a:octobercms:october:*:*:*:*:*:*:*:*:

cpe:2.3:a:octobercms:october:*:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→