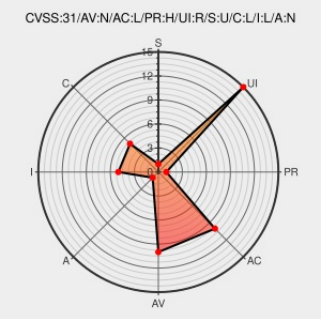
CVE-2020-11083

Published on: 07/14/2020 12:00:00 AM UTC

Last Modified on: 01/28/2023 01:49:00 AM UTC

CVE-2020-11083 - advisory for GHSA-w4pj-7p68-3vgv

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 1.0.466, a user with access to a markdown FormWidget that stores data persistently could create a stored XSS attack against themselves and any other users with access to the generated HTML from the field. This has been fixed in 1.0.466. For users of the RainLab.Blog plugin, this has also been fixed in 1.4.1.

CVE-2020-11083 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, < 1.0.466**

CVSS3 Score: 4.8 - MEDIUM

Attack Vector	Attack Complexity	Privileges Required	User Interaction
NETWORK	LOW	HIGH	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

Description	Tags	Link
October CMS Build 465 XSS / File Read / File Deletion / CSV Injection ≈ Packet Storm	packetstormsecurity.com text/html	MISC packetstormsecurity.com/files/158730/October-CMS-Build-465-XSS-F Read-File-Deletion-CSV-Injection.html
Add new backend.allow_unsafe_markdown permission · octobercms/october@9ecfb48 · GitHub	Patch Third Party Advisory github.com text/html	MISC github.com/octobercms/october/commit/9ecfb4867baae14a0d3f99f5b5c1e8a97
Stored XSS by authenticated backend user with access to markdown fields · Advisory · octobercms/october · GitHub	Patch Third Party Advisory github.com text/html	CONFIRM github.com/octobercms/october/security/advisories/GHSA-w4pj-7 3vgv
Implement support for backend.allow_unsafe_markdown and improve suppo… · rainlab/blog-plugin@6ae19a6 · GitHub	Patch Third Party Advisory github.com text/html	MISC github.com/rainlab/blog-plugin/commit/6ae19a6e16ef3ba730692bc899851342c858bb94
Full Disclosure: October CMS <= Build 465 Multiple Vulnerabilities - Arbitrary File Read	seclists.org text/html	FULLDISC 20200804 October CMS <= Build 465 Multiple Vulnerabilities - A File Read

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→

site. This site includes MITRE data granted under the following license.

CVE.report and Source URL Uptime Status status.cve.report