

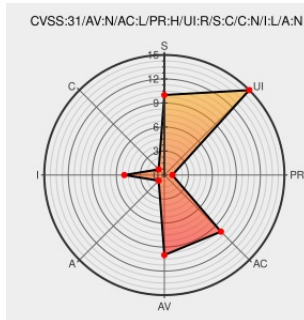


CVE-2020-5297

Published on: 06/03/2020 12:00:00 AM UTC

Last Modified on: 06/30/2022 02:46:00 PM UTC

CVE-2020-5297 - advisory for GHSA-9722-rr68-rfpg

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

Certain versions of [October](#) from [Octobercms](#) contain the following vulnerability:

In OctoberCMS (october/october composer package) versions from 1.0.319 and before 1.0.466, an attacker can exploit this vulnerability to upload jpg, jpeg, bmp, png, webp, gif, ico, css, js, woff, woff2, svg, ttf, eot, json, md, less, sass, scss, xml files to any directory of an October CMS server. The vulnerability is only exploitable by an authenticated backend user with the `cms.manage\_assets` permission. Issue has been patched in Build 466 (v1.0.466).

CVE-2020-5297 has been assigned by security-advisories@github.com to track the vulnerability - currently rated as **LOW** severity.

Affected Vendor/Software: **octobercms** - **october** version **>= 1.0.319, < 1.0.466**

CVSS3 Score: **2.7 - LOW**

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

CVSS2 Score: **4 - MEDIUM**

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

CVE References

Description	Tags	Link
Improve asset file path handling when moving assets · octobercms/october@6711dae · GitHub	Patch Third Party Advisory github.com text/html	MISC github.com/octobercms/october/commit/6711dae8ef70caf0e94cec434498012a2cc
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-File-Read-File-Deletion-CSV-Injection.html
Arbitrary Upload of Whitelisted File Types by authenticated backend user with cms.manage_assets permission · Advisory · octobercms/october · GitHub	Patch Third Party Advisory github.com text/html	CONFIRM github.com/octobercms/october/security/advisories/GHSA-9722-rr6f
Full Disclosure: October CMS <= Build 465 Multiple Vulnerabilities - Arbitrary File Read	seclists.org text/html	FULLDISC 20200804 October CMS <= Build 465 Multiple Vulnerabilities - Arbitrary 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

Social Mentions

Source	Title	Posted (UTC)
@RemotelyAlerts	Severity: ?? In OctoberCMS (october/october composer ... CVE-2020-5297 Link for more: alerts.remotelyrmm.com/CVE-2020-5297	2022-06-30 16:36:17

[← Previous ID](#)

[Next ID →](#)

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](#)