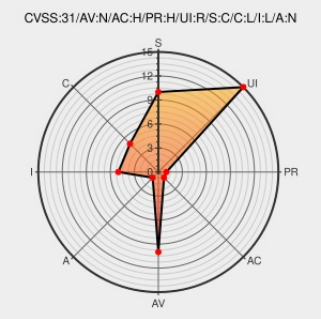
CVE-2020-5299

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

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

CVE-2020-5299 - advisory for GHSA-4rhm-m2fp-hx7q

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, any users with the ability to modify any data that could eventually be exported as a CSV file from the `ImportExportController` could potentially introduce a CSV injection into the data to cause the generated CSV export file to be malicious. This requires attackers to achieve the following before a successful attack can be completed: 1. Have found a vulnerability in the victims spreadsheet software of choice. 2. Control data that would potentially be exported through the `ImportExportController` by a theoretical victim. 3. Convince the victim to export above data as a CSV and run it in vulnerable spreadsheet software while also bypassing any sanity checks by said software. Issue has been patched in Build 466 (v1.0.466).

CVE-2020-5299 has been assigned by security-advisories@github.com to track the vulnerability - currently rated as MEDIUM severity.

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

CVSS3 Score: 5.1 - MEDIUM

Attack Vector	Attack Complexity	Privileges Required	User Interaction
NETWORK	HIGH	HIGH	REQUIRED
Scope	**Confidentiality Impact**	**Integrity Impact**	**Availability Impact**
CHANGED	LOW	LOW	LOW

CVSS2 Score: 4.6 - MEDIUM

Access Vector	Access Complexity	Authentication
NETWORK	HIGH	SINGLE
Confidentiality	**Integrity**	**Availability**

Confidentiality Impact	Integrity Impact	Availability Impact
PARTIAL	PARTIAL	PARTIAL

CVE References

Description	Tags	Link
Temporary workaround until the L6 upgrade can be merged in to use lea… · octobercms/october@802d8c8 · GitHub	Patch, Third Party Advisory, github.com, text/html	MISC github.com/octobercms/october/commit/802d8c8e09a2b342649393edb6d3ceb958
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-File-Deletion-CSV-Injection.html
Potential CSV Injection vector · Advisory · octobercms/october · GitHub	Patch, Third Party Advisory, github.com, text/html	CONFIRM github.com/octobercms/october/security/advisories/GHSA-4rhm-m2
Temporary workaround until the L6 upgrade can be merged in to use lea… · octobercms/library@c84bf03 · GitHub	Patch, Third Party Advisory, github.com, text/html	MISC github.com/octobercms/library/commit/c84bf03f506052c848f2fddc05f24be631427a
Full Disclosure: October CMS <= Build 465 Multiple Vulnerabilities - Arbitrary File Read	seclists.org, text/html	FULLDISC 20200804 October CMS <= Build 465 Multiple Vulnerabilities - Arbit File Read

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-2020-5299 | Link for more: alerts.remotelyrmm.com/CVE-2020-5299	2022-06-30 16:35:41

← Previous ID

Next ID→