

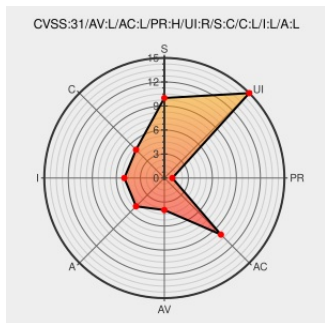


CVE-2020-15247

Published on: 11/23/2020 12:00:00 AM UTC

Last Modified on: 11/18/2021 04:28:00 PM UTC

CVE-2020-15247 - advisory for GHSA-94vp-rmqv-5875

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

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

October is a free, open-source, self-hosted CMS platform based on the Laravel PHP Framework. In October CMS from version 1.0.319 and before version 1.0.469, an authenticated backend user with the `cms.manage_pages`, `cms.manage_layouts`, or `cms.manage_partials` permissions who would normally not be permitted to provide PHP code

to be executed by the CMS due to `cms.enableSafeMode` being enabled is able to write specific Twig code to escape the Twig sandbox and execute arbitrary PHP. This is not a problem for anyone that trusts their users with those permissions to normally write & manage PHP within the CMS by not having `cms.enableSafeMode` enabled, but would be a problem for anyone relying on `cms.enableSafeMode` to ensure that users with those permissions in production do not have access to write & execute arbitrary PHP. Issue has been patched in Build 469 (v1.0.469) and v1.1.0.

CVE-2020-15247 has been assigned by [security-advisories@github.com](#) to track the vulnerability - currently rated as **MEDIUM** severity.

Affected Vendor/Software: **octobercms** - **october** version $\geq 1.0.319$, $< 1.0.469$

CVSS3 Score: **5.2 - MEDIUM**

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

CVSS2 Score: **4.4 - MEDIUM**

Access Vector	Access Complexity	Authentication
LOCAL	MEDIUM	NONE

Confidentiality Impact

Integrity Impact

Availability Impact

PARTIAL

PARTIAL

PARTIAL

CVE References

Description

Tags

Link

Twig Sandbox Escape by authenticated users with access to editing CMS templates when safemode is enabled. · Advisory · octobercms/october · GitHub

Third Party Advisory

github.com

text/html

 CONFIRM github.com/octobercms/october/security/advisories/GHSA-94vp-rmqv-58

Security fixes for v1.0.469 · octobercms/october@4c650bb · GitHub

Patch

Third Party Advisory

github.com

text/html

 MISC github.com/octobercms/october/commit/4c650bb775ab849e48202a4923bac93bd74f9c

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: ?? | October is a free, open-source, self-hos... | CVE-2020-15247 | Link for more: alerts.remotelyrmm.com/CVE-2020-15247

2021-11-18 18:12:41

← 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](#)