



CVE-2020-15189

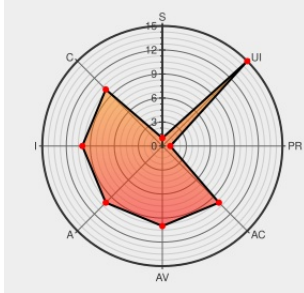
Published on: 09/18/2020 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:23:40 PM UTC

CVE-2020-15189 - advisory for GHSA-6r2f-p68g-m433

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

CVSS:31/AV:N/AC:L/PR:H/UI:R/S:U/C:H/I:H/A:H



Certain versions of [Soy Cms](#) from [Brassica](#) contain the following vulnerability:

SOY CMS 3.0.2 and earlier is affected by Remote Code Execution (RCE) using Unrestricted File Upload. Cross-Site Scripting(XSS) vulnerability that was used in CVE-2020-15183 can be used to increase impact by redirecting the administrator to access a specially crafted page. This vulnerability is caused by insecure configuration in elFinder. This is fixed in version 3.0.2.328.

CVE-2020-15189 has been assigned by security-advisories@github.com to track the vulnerability - currently rated as **HIGH** severity.

Affected Vendor/Software: inunosini - **soycms** version < **3.0.2.328**

CVSS3 Score: **7.2 - HIGH**

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

CVSS2 Score: **6.5 - MEDIUM**

Access Vector	Access Complexity	Authentication
NETWORK	LOW	SINGLE
Confidentiality Impact	Integrity Impact	Availability Impact
PARTIAL	PARTIAL	PARTIAL

CVE References

Description	Tags	Link
-------------	------	------

Remote Code Execution (RCE) in SoyCMS · Issue #9 · inunosinsi/soycms · GitHub	Exploit Mitigation Third Party Advisory github.com text/html	 MISC github.com/inunosinsi/soycms/issues/9
(CVE-2020-15189) SoyCMS: Remote Code Execution using unrestricted file upload - YouTube	Exploit Third Party Advisory youtu.be text/html	 MISC youtu.be/FWIDFNXmr9g
Fix RCE: Block PHP extension upload by stypr · Pull Request #14 · inunosinsi/soycms · GitHub	Patch Third Party Advisory github.com text/html	 MISC github.com/inunosinsi/soycms/pull/14/commits/e4ef00677ed52f9e5a5fcfc56b797f5412b5d59
Fix RCE: Block PHP extension upload by stypr · Pull Request #14 · inunosinsi/soycms · GitHub	Patch Third Party Advisory github.com text/html	 MISC github.com/inunosinsi/soycms/pull/14
Remote Code Execution in SOY CMS · Advisory · inunosinsi/soycms · GitHub	Third Party Advisory github.com text/html	 CONFIRM github.com/inunosinsi/soycms/security/advisories/GHSA-6r2f-p68g-m433

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	Brassica	Soy Cms	All	All	All	All
Application	Brassica	Soy Cms	All	All	All	All
cpe:2.3:a:brassica:soy_cms:*****:						
cpe:2.3:a:brassica:soy_cms:*****:						

No vendor comments have been submitted for this CVE

[← Previous ID](#)

[Next ID →](#)

this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, 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](#)