



CVE-2020-15182

[MITRE](#)[NVD](#)[CVE.ORG](#)[JSON API](#)[Print: PDF](#)

Summary

CVE	CVE-2020-15182
State	PUBLIC
Assigner	security-advisories@github.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2020-09-17 20:15:00 UTC
Updated	2020-09-23 20:20:00 UTC
Description	The SOY Inquiry component of SOY CMS is affected by Cross-site Request Forgery (CSRF) and Remote Code Execution

Risk And Classification

Problem Types: CWE-352 | CWE-22

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Soy Cms Project	Soy Cms	All	All	All	All
Application	Soy Cms Project	Soy Cms	All	All	All	All
Application	Soy Inquiry Project	Soy Inquiry	All	All	All	All
Application	Soy Inquiry Project	Soy Inquiry	All	All	All	All

References

Reference	Source	Link	Tags
Fix CSRF and Directory Traversal by stypr · Pull Request #15 · inunosinsi/soycms · GitHub	MISC	github.com	Patch
(CVE-2020-15182) SoyCMS: CSRF leading to RCE - YouTube	MISC	youtu.be	Explo
Cross-site Request Forgery (CSRF) leading to RCE in SOY CMS · Advisory · inunosinsi/soycms · GitHub	CONFIRM	github.com	Third
CVE Program record	CVE.ORG	www.cve.org	cano
NVD vulnerability detail	NVD	nvd.nist.gov	cano

No vendor comments have been submitted for this CVE.

There are currently no legacy QID mappings associated with this CVE.

© [CVE.report](#) 2026 |

Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to 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](#).

Free CVE JSON API [cve.report/api](#)

CVE.report and Source URL Uptime Status [status.cve.report](#)