



# CVE-2015-8766

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

## Summary

<b>CVE</b>	CVE-2015-8766
<b>State</b>	PUBLIC
<b>Assigner</b>	cve@mitre.org
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2016-01-08 21:59:00 UTC
<b>Updated</b>	2020-10-29 22:15:00 UTC
<b>Description</b>	Multiple cross-site scripting (XSS) vulnerabilities in content/content.systempreferences.php in Symphony CMS before 2.6.4

## Risk And Classification

**Problem Types:** CWE-79

## NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	<a href="#">Getsymphony</a>	<a href="#">Symphony</a>	All	All	All	All

## References

Reference	Source	Link	Ta
CVE-2015-8766 - Reflected Cross-Site Scripting (XSS) in Symphony CMS	MISC	<a href="#">cybersecurityworks.com</a>	
Full Disclosure: Symphony 2.6.3 – Multiple Persistent Cross-Site Scripting Vulnerabilities	FULLDISC	<a href="#">seclists.org</a>	Ex
Sanitize the POST for the system/preferences/ · symphonycms/symphony-2@651e150 · GitHub	CONFIRM	<a href="#">github.com</a>	
Release Details – Release History – Download – Symphony.	CONFIRM	<a href="#">www.getsymphony.com</a>	Pa
CVE Program record	CVE.ORG	<a href="#">www.cve.org</a>	ca
NVD vulnerability detail	NVD	<a href="#">nvd.nist.gov</a>	ca

No vendor comments have been submitted for this CVE.

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

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](#)