



CVE-2011-4340

Published on: 02/12/2012 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:23:12 PM UTC

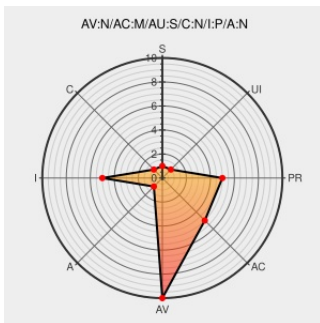
CVE-2011-4340

Source: Mitre

Source: NIST

CVE.ORG

Print: PDF



Certain versions of [Symphony Cms](#) from [Symphony-cms](#) contain the following vulnerability:

Multiple cross-site scripting (XSS) vulnerabilities in Symphony CMS 2.2.3 and possibly other versions before 2.2.4 allow remote authenticated users with Author privileges to inject arbitrary web script or HTML via (1) the profile parameter to extensions/profiledevkit/content/content.profile.php, as demonstrated

via requests to (a) the default URI, (b) about/, or (c) drafts/; or (2) the filter parameter in symphony/lib/core/class.symphony.php, as demonstrated via requests to (d) symphony/publish/comments or (e) symphony/publish/images. NOTE: some of these details are obtained from third party information.

CVE-2011-4340 has been assigned by secalert@redhat.com to track the vulnerability

CVSS2 Score: **3.5 - LOW**

Access
Vector

NETWORK

Access
Complexity

MEDIUM

Authentication

SINGLE

Confidentiality
Impact

NONE

Integrity
Impact

PARTIAL

Availability
Impact

NONE

CVE References

Description

Tags

Link

Release Details – Release History – Download – Symphony.

Patch
[web.archive.org](#)
text/html

Inactive Link **Not Archived**

CONFIRM [symphony-cms.com/download/releases/version/2.2.4/](#)

Netsparker, False Positive Free Web Application Security Scanner - Mavituna Security

[www.mavitunasecurity.com](#)
text/html

MISC [www.mavitunasecurity.com/xss-and-sql-injection-vulnerabilities-in-symphony-cms/](#)

No Description Provided

[www.osvdb.org](#)

OSVDB 76882

Inactive Link Not Archived

IBM X-Force Exchange

exchange.xforce.ibmcloud.com
text/html

XF symphony-multiple-xss(71106)

oss-security - Re: CVE-request: Symphony CMS
Multiple Cross-Site Scripting and SQL Injection
Vulnerabilities (NS-11-008)

www.openwall.com
text/html

MLIST [oss-security] 20111122 Re: CVE-request:
Symphony CMS Multiple Cross-Site Scripting and SQL
Injection Vulnerabilities (NS-11-008)

Security Advisory SA46663 - Symphony CMS
Multiple Cross-Site Scripting and SQL Injection
Vulnerabilities - Secunia

Vendor Advisory
web.archive.org
text/html

SECUNIA 46663

No Description Provided

www.osvdb.org

OSVDB 76883

Inactive Link Not Archived

Bugtraq: XSS and SQL Injection Vulnerabilities
on Symphony CMS 2.2.3

seclists.org
text/html

BUGTRAQ 20111101 XSS and SQL Injection
Vulnerabilities on Symphony CMS 2.2.3

Symphony CMS 2.2.3 Cross Site Scripting / SQL
Injection ~ Packet Storm

packetstormsecurity.org
text/html

MISC
packetstormsecurity.org/files/view/106493/symphonycms-
sqlxss.txt

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	Symphony-cms	Symphony Cms	2.2.3	All	All	All
Application	Symphony-cms	Symphony Cms	2.2.3	All	All	All
cpe:2.3:a:symphony-cms:symphony_cms:2.2.3:****:****:						
cpe:2.3:a:symphony-cms:symphony_cms:2.2.3:****:****:						

No vendor comments have been submitted for this CVE

[← Previous ID](#)

[Next ID →](#)

© CVE.report 2023   |

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](#).

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