



CVE-2011-4958

Published on: 04/08/2014 12:00:00 AM UTC

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

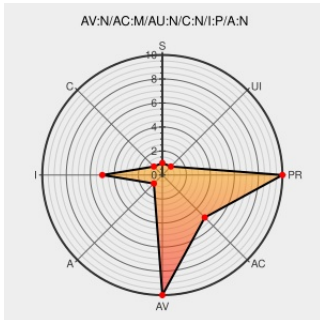
CVE-2011-4958

Source: Mitre

Source: NIST

CVE.ORG

Print: PDF



Certain versions of Silverstripe from Silverstripe contain the following vulnerability:

Cross-site scripting (XSS) vulnerability in the process function in SSViewer.php in SilverStripe before 2.3.13 and 2.4.x before 2.4.6 allows remote attackers to inject arbitrary web script or HTML via the QUERY_STRING to template placeholders, as demonstrated by a request to (1) admin/reports/, (2) admin/comments/, (3) admin/, (4) admin/show/, (5) admin/assets/, and (6) admin/security/.

CVE-2011-4958 has been assigned by secalert@redhat.com to track the vulnerability

CVSS2 Score: 4.3 - MEDIUM

Access Vector

Access Complexity

Authentication

NETWORK

MEDIUM

NONE

Confidentiality Impact

Integrity Impact

Availability Impact

NONE

PARTIAL

NONE

CVE References

Description

Tags

Link

BUGFIX Escaping base URLs for anchor links rewritten by SSViewer::pro...
silverstripe/silverstripe-framework@52a895f · GitHub

Exploit
Patch
github.com
text/html

CONFIRM
github.com/silverstripe/sapphire/commit/52a895f

AfterMarket.pl :: domena rul3z.de

Exploit
www.rul3z.de
text/html

MISC www.rul3z.de/advisories/SSCHADV2011-024.txt

No Description Provided

osvdb.org

OSVDB 76258

Inactive Link Not Archived

2.4.6 - Changelogs - Sapphire - SilverStripe

web.archive.org

CONFIRM

2.3.12 - Changelogs - Sapphire - SilverStripe Documentation	web.archive.org text/html Inactive Link Not Archived	CONFIRM doc.silverstripe.org/sapphire/en/trunk/changelogs/2.4.6
SilverStripe URL Cross-Site Scripting Vulnerability - Secunia.com	Vendor Advisory web.archive.org text/html	SECUNIA 46390
2.3.12 - Changelogs - Sapphire - SilverStripe Documentation	web.archive.org text/html Inactive Link Not Archived	CONFIRM doc.silverstripe.org/sapphire/en/trunk/changelogs/2.3.12
BUGFIX Respecting SSViewer::\$options["rewriteHashlinks"] in SSViewer: ... · silverstripe/silverstripe-framework@bdd6391 · GitHub	Exploit Patch github.com text/html	CONFIRM github.com/silverstripe/sapphire/commit/bdd6391
BUGFIX Escaping base URLs for anchor links rewritten by SSViewer::pro... · silverstripe/silverstripe-framework@16c3235 · GitHub	Exploit Patch github.com text/html	CONFIRM github.com/silverstripe/sapphire/commit/16c3235
SecurityFocus	web.archive.org text/html Inactive Link Not Archived	BUGTRAQ 20111008 SilverStripe 2.4.5 Multiple backend Cross-site scripting vulnerabilities

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	Silverstripe	Silverstripe	2.3.0	All	All	All
Application	Silverstripe	Silverstripe	2.3.0	rc1	All	All
Application	Silverstripe	Silverstripe	2.3.0	rc2	All	All
Application	Silverstripe	Silverstripe	2.3.0	rc3	All	All
Application	Silverstripe	Silverstripe	2.3.1	All	All	All
Application	Silverstripe	Silverstripe	2.3.1	rc1	All	All
Application	Silverstripe	Silverstripe	2.3.1	rc2	All	All
Application	Silverstripe	Silverstripe	2.3.10	All	All	All
Application	Silverstripe	Silverstripe	2.3.11	All	All	All
Application	Silverstripe	Silverstripe	2.3.2	All	All	All
Application	Silverstripe	Silverstripe	2.3.3	All	All	All
Application	Silverstripe	Silverstripe	2.3.4	All	All	All
Application	Silverstripe	Silverstripe	2.3.5	All	All	All
Application	Silverstripe	Silverstripe	2.3.6	All	All	All
Application	Silverstripe	Silverstripe	2.3.7	All	All	All

cpe:2.3:a:silverstripe:silverstripe:2.3.0:rc2:*****:
cpe:2.3:a:silverstripe:silverstripe:2.3.0:rc3:*****:
cpe:2.3:a:silverstripe:silverstripe:2.3.1:*****:
cpe:2.3:a:silverstripe:silverstripe:2.3.1:rc1:*****:
cpe:2.3:a:silverstripe:silverstripe:2.3.1:rc2:*****:
cpe:2.3:a:silverstripe:silverstripe:2.3.10:*****:
cpe:2.3:a:silverstripe:silverstripe:2.3.11:*****:
cpe:2.3:a:silverstripe:silverstripe:2.3.2:*****:
cpe:2.3:a:silverstripe:silverstripe:2.3.3:*****:
cpe:2.3:a:silverstripe:silverstripe:2.3.4:*****:
cpe:2.3:a:silverstripe:silverstripe:2.3.5:*****:
cpe:2.3:a:silverstripe:silverstripe:2.3.6:*****:
cpe:2.3:a:silverstripe:silverstripe:2.3.7:*****:
cpe:2.3:a:silverstripe:silverstripe:2.3.8:*****:
cpe:2.3:a:silverstripe:silverstripe:2.3.9:*****:
cpe:2.3:a:silverstripe:silverstripe:2.4.0:*****:
cpe:2.3:a:silverstripe:silverstripe:2.4.1:*****:
cpe:2.3:a:silverstripe:silverstripe:2.4.2:*****:
cpe:2.3:a:silverstripe:silverstripe:2.4.3:*****:
cpe:2.3:a:silverstripe:silverstripe:2.4.4:*****:
cpe:2.3:a:silverstripe:silverstripe:2.4.5:*****:
cpe:2.3:a:silverstripe:silverstripe:2.3.0:*****:
cpe:2.3:a:silverstripe:silverstripe:2.3.0:rc1:*****:
cpe:2.3:a:silverstripe:silverstripe:2.3.0:rc2:*****:
cpe:2.3:a:silverstripe:silverstripe:2.3.0:rc3:*****:
cpe:2.3:a:silverstripe:silverstripe:2.3.1:*****:
cpe:2.3:a:silverstripe:silverstripe:2.3.1:rc1:*****:
cpe:2.3:a:silverstripe:silverstripe:2.3.1:rc2:*****:
cpe:2.3:a:silverstripe:silverstripe:2.3.10:*****:

cpe:2.3:a:silverstripe:silverstripe:2.3.11:*****:
cpe:2.3:a:silverstripe:silverstripe:2.3.2:*****:
cpe:2.3:a:silverstripe:silverstripe:2.3.3:*****:
cpe:2.3:a:silverstripe:silverstripe:2.3.4:*****:
cpe:2.3:a:silverstripe:silverstripe:2.3.5:*****:
cpe:2.3:a:silverstripe:silverstripe:2.3.6:*****:
cpe:2.3:a:silverstripe:silverstripe:2.3.7:*****:
cpe:2.3:a:silverstripe:silverstripe:2.3.8:*****:
cpe:2.3:a:silverstripe:silverstripe:2.3.9:*****:
cpe:2.3:a:silverstripe:silverstripe:2.4.0:*****:
cpe:2.3:a:silverstripe:silverstripe:2.4.1:*****:
cpe:2.3:a:silverstripe:silverstripe:2.4.2:*****:
cpe:2.3:a:silverstripe:silverstripe:2.4.3:*****:
cpe:2.3:a:silverstripe:silverstripe:2.4.4:*****:
cpe:2.3:a:silverstripe:silverstripe:2.4.5:*****:
cpe:2.3:a:silverstripe:silverstripe:*****:

No vendor comments have been submitted for this CVE

[← Previous ID](#)

[Next ID→](#)