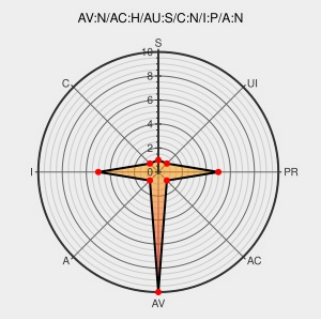
CVE-2013-0227

Published on: 03/19/2013 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:28:41 PM UTC

CVE-2013-0227

Source: Mitre | Source: NIST | CVE.ORG | Print: PDF



Certain versions of Drupal from Drupal contain the following vulnerability:

Cross-site scripting (XSS) vulnerability in the Search API Sorts module 7.x-1.x before 7.x-1.4 for Drupal allows remote authenticated users with certain roles to inject arbitrary web script or HTML via unspecified field labels.

CVE-2013-0227 has been assigned by secalert@redhat.com to track the vulnerability

CVSS2 Score: 2.1 - LOW

Access Vector	Access Complexity	Authentication
NETWORK	HIGH	SINGLE
Confidentiality Impact	**Integrity Impact**	**Availability Impact**
NONE	PARTIAL	NONE

CVE References

Description	Tags	Link
SA-CONTRIB-2013-010 - Search API sorts - Cross Site Scripting (XSS) | drupal.org	Patch, Vendor Advisory, drupal.org, text/html	MISC drupal.org/node/1896782
oss-security - Re: CVE request for Drupal contributed modules	www.openwall.com, text/html	MLIST [oss-security] 20130124 Re: CVE request for Drupal contributed modules
search_api_sorts 7.x-1.4 | drupal.org	Patch, drupal.org, text/html	CONFIRM drupal.org/node/1896756
Log in | Drupal.org	drupalcode.org, text/html	CONFIRM drupalcode.org/project/search_api_sorts.git/commitdiff/f6cbf47

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	Drupal	Drupal	-	All	All	All
Application	Drupal	Drupal	-	All	All	All
Application	Mathijs Koenraadt	Search Api Sorts	7.x-1.0	All	All	All
Application	Mathijs Koenraadt	Search Api Sorts	7.x-1.1	All	All	All
Application	Mathijs Koenraadt	Search Api Sorts	7.x-1.2	All	All	All
Application	Mathijs Koenraadt	Search Api Sorts	7.x-1.3	All	All	All
Application	Mathijs Koenraadt	Search Api Sorts	7.x-1.x	dev	All	All
Application	Mathijs Koenraadt	Search Api Sorts	7.x-1.0	All	All	All
Application	Mathijs Koenraadt	Search Api Sorts	7.x-1.1	All	All	All
Application	Mathijs Koenraadt	Search Api Sorts	7.x-1.2	All	All	All
Application	Mathijs Koenraadt	Search Api Sorts	7.x-1.3	All	All	All
Application	Mathijs Koenraadt	Search Api Sorts	7.x-1.x	dev	All	All

cpe:2.3:a:drupal:drupal:-:*:*:*:*:*:*:*:

cpe:2.3:a:drupal:drupal:-:*:*:*:*:*:*:*:

cpe:2.3:a:mathijs_koenraadt:search_api_sorts:7.x-1.0:*:*:*:*:*:*:*:

cpe:2.3:a:mathijs_koenraadt:search_api_sorts:7.x-1.1:*:*:*:*:*:*:*:

cpe:2.3:a:mathijs_koenraadt:search_api_sorts:7.x-1.2:*:*:*:*:*:*:*:

cpe:2.3:a:mathijs_koenraadt:search_api_sorts:7.x-1.3:*:*:*:*:*:*:*:

cpe:2.3:a:mathijs_koenraadt:search_api_sorts:7.x-1.x:dev:*:*:*:*:*:*:

cpe:2.3:a:mathijs_koenraadt:search_api_sorts:7.x-1.0:*:*:*:*:*:*:*:

cpe:2.3:a:mathijs_koenraadt:search_api_sorts:7.x-1.1:*:*:*:*:*:*:*:

cpe:2.3:a:mathijs_koenraadt:search_api_sorts:7.x-1.2:*:*:*:*:*:*:*:

cpe:2.3:a:mathijs_koenraadt:search_api_sorts:7.x-1.3:*:*:*:*:*:*:*:

cpe:2.3:a:mathijs_koenraadt:search_api_sorts:7.x-1.x:dev:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→