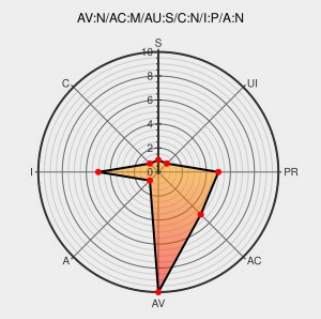
CVE-2014-9346

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

Last Modified on: 03/23/2021 11:25:59 PM UTC

CVE-2014-9346

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



Certain versions of Hierarchical Select from Hierarchical Select Project contain the following vulnerability:

Multiple cross-site scripting (XSS) vulnerabilities in the Hierarchical Select module 6.x-3.x before 6.x-3.9 for Drupal allow remote authenticated users with certain permissions to inject arbitrary web script or HTML via vectors related to the (1) taxonomy term title for instances with Save term lineage enabled or (2) entity type fields.

CVE-2014-9346 has been assigned by cve@mitre.org to track the vulnerability

CVSS2 Score: 3.5 - LOW

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

CVE References

Description	Tags	Link
SA-CONTRIB-2014-117 - Hierarchical Select - Cross Site Scripting (XSS) | Drupal.org	Vendor Advisory, www.drupal.org, text/html	MISC www.drupal.org/node/2386615
IBM X-Force Exchange	exchange.xforce.ibmcloud.com, text/html	XF hierarchicalselect-hierarchicalselect-xss(99136)
Security Advisory SA60511 - Drupal Hierarchical Select Module Two Script Insertion Vulnerabilities - Secunia	web.archive.org, text/html	SECUNIA 60511
hierarchical_select 6.x-3.9 | Drupal.org	Patch, www.drupal.org, text/html	CONFIRM www.drupal.org/node/2385933

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	Hierarchical Select Project	Hierarchical Select	6.x-3.0	All	All	All
Application	Hierarchical Select Project	Hierarchical Select	6.x-3.1	All	All	All
Application	Hierarchical Select Project	Hierarchical Select	6.x-3.2	All	All	All
Application	Hierarchical Select Project	Hierarchical Select	6.x-3.3	All	All	All
Application	Hierarchical Select Project	Hierarchical Select	6.x-3.4	All	All	All
Application	Hierarchical Select Project	Hierarchical Select	6.x-3.5	All	All	All
Application	Hierarchical Select Project	Hierarchical Select	6.x-3.6	All	All	All
Application	Hierarchical Select Project	Hierarchical Select	6.x-3.7	All	All	All
Application	Hierarchical Select Project	Hierarchical Select	6.x-3.8	All	All	All
Application	Hierarchical Select Project	Hierarchical Select	6.x-3.x	dev	All	All
Application	Hierarchical Select Project	Hierarchical Select	6.x-3.0	All	All	All
Application	Hierarchical Select Project	Hierarchical Select	6.x-3.1	All	All	All
Application	Hierarchical Select Project	Hierarchical Select	6.x-3.2	All	All	All
Application	Hierarchical Select Project	Hierarchical Select	6.x-3.3	All	All	All
Application	Hierarchical Select Project	Hierarchical Select	6.x-3.4	All	All	All
Application	Hierarchical Select Project	Hierarchical Select	6.x-3.5	All	All	All
Application	Hierarchical Select Project	Hierarchical Select	6.x-3.6	All	All	All
Application	Hierarchical Select Project	Hierarchical Select	6.x-3.7	All	All	All
Application	Hierarchical Select Project	Hierarchical Select	6.x-3.8	All	All	All
Application	Hierarchical Select Project	Hierarchical Select	6.x-3.x	dev	All	All

cpe:2.3:a:hierarchical_select_project:hierarchical_select:6.x-3.0:*:*:*:*:drupal:*:*:

cpe:2.3:a:hierarchical_select_project:hierarchical_select:6.x-3.1:*:*:*:*:drupal:*:*:

cpe:2.3:a:hierarchical_select_project:hierarchical_select:6.x-3.2:*:*:*:*:drupal:*:*:

cpe:2.3:a:hierarchical_select_project:hierarchical_select:6.x-3.3:*:*:*:*:drupal:*:*:

cpe:2.3:a:hierarchical_select_project:hierarchical_select:6.x-3.4:*:*:*:*:drupal:*:*:

cpe:2.3:a:hierarchical_select_project:hierarchical_select:6.x-3.5:*:*:*:*:drupal:*:*:

cpe:2.3:a:hierarchical_select_project:hierarchical_select:6.x-3.6:*:*:*:*:drupal:*:*:

cpe:2.3:a:hierarchical_select_project:hierarchical_select:6.x-3.7:*:*:*:*:drupal:*:*:

cpe:2.3:a:hierarchical_select_project:hierarchical_select:6.x-3.8:*:*:*:*:drupal:*:*:

cpe:2.3:a:hierarchical_select_project:hierarchical_select:6.x-3.x:dev:*:*:*:drupal:*:*:

cpe:2.3:a:hierarchical_select_project:hierarchical_select:6.x-3.0:*:*:*:*:drupal:*:*:

cpe:2.3:a:hierarchical_select_project:hierarchical_select:6.x-3.1:*:*:*:*:drupal:*:*:

cpe:2.3:a:hierarchical_select_project:hierarchical_select:6.x-3.2:*:*:*:*:drupal:*:*:

cpe:2.3:a:hierarchical_select_project:hierarchical_select:6.x-3.3:*:*:*:*:drupal:*:*:

cpe:2.3:a:hierarchical_select_project:hierarchical_select:6.x-3.4:*:*:*:*:drupal:*:*:

cpe:2.3:a:hierarchical_select_project:hierarchical_select:6.x-3.5:*:*:*:*:drupal:*:*:

cpe:2.3:a:hierarchical_select_project:hierarchical_select:6.x-3.6:*:*:*:*:drupal:*:*:

cpe:2.3:a:hierarchical_select_project:hierarchical_select:6.x-3.7:*:*:*:*:drupal:*:*:

cpe:2.3:a:hierarchical_select_project:hierarchical_select:6.x-3.8:*:*:*:*:drupal:*:*:

cpe:2.3:a:hierarchical_select_project:hierarchical_select:6.x-3.x:dev:*:*:*:drupal:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→