CVE-2013-1906

MITRE | NVD | CVE.ORG | JSON API | Print: PDF

Summary

CVE	CVE-2013-1906
State	PUBLIC
Assigner	secalert@redhat.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2013-06-24 16:55:00 UTC
Updated	2013-06-25 15:12:00 UTC
Description	Cross-site scripting (XSS) vulnerability in the Rules module 7.x-2.x before 7.x-2.3 for Drupal allows remote authenticated us

Risk And Classification

Problem Types: CWE-79

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Drupal	Drupal	-	All	All	All
Application	Drupal	Drupal	-	All	All	All
Application	Wolfgang Ziegler	Rules	7.x-2.0	All	All	All
Application	Wolfgang Ziegler	Rules	7.x-2.0-beta1	All	All	All
Application	Wolfgang Ziegler	Rules	7.x-2.0-beta2	All	All	All
Application	Wolfgang Ziegler	Rules	7.x-2.0-beta3	All	All	All
Application	Wolfgang Ziegler	Rules	7.x-2.0-rc1	All	All	All
Application	Wolfgang Ziegler	Rules	7.x-2.0-rc2	All	All	All
Application	Wolfgang Ziegler	Rules	7.x-2.1	All	All	All
Application	Wolfgang Ziegler	Rules	7.x-2.2	All	All	All
Application	Wolfgang Ziegler	Rules	7.x-2.0	All	All	All
Application	Wolfgang Ziegler	Rules	7.x-2.0-beta1	All	All	All
Application	Wolfgang Ziegler	Rules	7.x-2.0-beta2	All	All	All
Application	Wolfgang Ziegler	Rules	7.x-2.0-beta3	All	All	All
Application	Wolfgang Ziegler	Rules	7.x-2.0-rc1	All	All	All
Application	Wolfgang Ziegler	Rules	7.x-2.0-rc2	All	All	All
Application	Wolfgang Ziegler	Rules	7.x-2.1	All	All	All

Application	Wolfgang Ziegler	Rules	7.x-2.2	All	All	All

References

Reference	Source	Link	Tags
rules 7.x-2.3 | drupal.org	CONFIRM	drupal.org	
About Secunia Research | Flexera	SECUNIA	secunia.com	Vendor Advisory
SA-CONTRIB-2013-037 - Rules - Cross Site Scripting (XSS) | drupal.org	MISC	drupal.org	
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical, analysis

No vendor comments have been submitted for this CVE.

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

Free CVE JSON API cve.report/api

CVE.report and Source URL Uptime Status **status.cve.report**