



CVE-2012-1654

[MITRE](#)[NVD](#)[CVE.ORG](#)[JSON API](#)[Print: PDF](#)

Summary

CVE	CVE-2012-1654
State	PUBLIC
Assigner	secalert@redhat.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2012-09-18 20:55:00 UTC
Updated	2012-12-20 05:00:00 UTC
Description	Multiple cross-site scripting (XSS) vulnerabilities in the Data module 6.x-1.x before 6.x-1.0 and 7.x-1.x before 7.x-1.0-alpha6

Risk And Classification

Problem Types: CWE-79

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Alex Barth	Data	6.x-1.0	alpha1	All	All
Application	Alex Barth	Data	6.x-1.0	alpha10	All	All
Application	Alex Barth	Data	6.x-1.0	alpha11	All	All
Application	Alex Barth	Data	6.x-1.0	alpha12	All	All
Application	Alex Barth	Data	6.x-1.0	alpha13	All	All
Application	Alex Barth	Data	6.x-1.0	alpha14	All	All
Application	Alex Barth	Data	6.x-1.0	alpha2	All	All
Application	Alex Barth	Data	6.x-1.0	alpha3	All	All
Application	Alex Barth	Data	6.x-1.0	alpha4	All	All
Application	Alex Barth	Data	6.x-1.0	alpha5	All	All
Application	Alex Barth	Data	6.x-1.0	alpha6	All	All
Application	Alex Barth	Data	6.x-1.0	alpha7	All	All
Application	Alex Barth	Data	6.x-1.0	alpha8	All	All
Application	Alex Barth	Data	6.x-1.0	alpha9	All	All
Application	Alex Barth	Data	6.x-1.x	dev	All	All
Application	Alex Barth	Data	7.x-1.0	alpha1	All	All
Application	Alex Barth	Data	7.x-1.0	alpha2	All	All

Application	Alex Barth	Data	7.x-1.x	dev	All	All
Application	Alex Barth	Data	6.x-1.0	alpha1	All	All
Application	Alex Barth	Data	6.x-1.0	alpha10	All	All
Application	Alex Barth	Data	6.x-1.0	alpha11	All	All
Application	Alex Barth	Data	6.x-1.0	alpha12	All	All
Application	Alex Barth	Data	6.x-1.0	alpha13	All	All
Application	Alex Barth	Data	6.x-1.0	alpha14	All	All
Application	Alex Barth	Data	6.x-1.0	alpha2	All	All
Application	Alex Barth	Data	6.x-1.0	alpha3	All	All
Application	Alex Barth	Data	6.x-1.0	alpha4	All	All
Application	Alex Barth	Data	6.x-1.0	alpha5	All	All
Application	Alex Barth	Data	6.x-1.0	alpha6	All	All
Application	Alex Barth	Data	6.x-1.0	alpha7	All	All
Application	Alex Barth	Data	6.x-1.0	alpha8	All	All
Application	Alex Barth	Data	6.x-1.0	alpha9	All	All
Application	Alex Barth	Data	6.x-1.x	dev	All	All
Application	Alex Barth	Data	7.x-1.0	alpha1	All	All
Application	Alex Barth	Data	7.x-1.0	alpha2	All	All
Application	Alex Barth	Data	7.x-1.x	dev	All	All
Application	Drupal	Drupal	-	All	All	All
Application	Drupal	Drupal	-	All	All	All

References						
Reference				Source	Link	Tags
Drupal Data 6.x-1.0 XSS Vulnerability Mad Irish . net				MISC	www.madirish.net	
oss-security - CVE's for Drupal Contrib 2012 001 through 057 (67 new CVE assignments)				MLIST	www.openwall.com	
Log in Drupal.org				CONFIRM	drupalcode.org	
79854				OSVDB	www.osvdb.org	
data 6.x-1.1 drupal.org				CONFIRM	drupal.org	Patch
data 7.x-1.0-alpha3 drupal.org				CONFIRM	drupal.org	Patch
Log in Drupal.org				CONFIRM	drupalcode.org	
Security Advisory SA48326 - Drupal Data Module Title Script Insertion Vulnerability - Secunia				SECUNIA	secunia.com	Vendor
Drupal Data Module Cross Site Scripting Vulnerability				BID	www.securityfocus.com	
SA-CONTRIB-2012-030 - Data - Cross Site Scripting (XSS) drupal.org				MISC	drupal.org	Vendor
CVE Program record				CVE.ORG	www.cve.org	canonical

No vendor comments have been submitted for this CVE.

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

© [CVE.report](https://cve.report) 2026 |

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](https://mitre.org) and the authoritative source of CVE content is [MITRE's CVE web site](https://mitre.org/cve). This site includes MITRE data granted under the following [license](#).

Free CVE JSON API cve.report/api

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