



CVE-2012-2075

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

Summary

CVE	CVE-2012-2075
State	PUBLIC
Assigner	secalert@redhat.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2012-08-14 23:55:00 UTC
Updated	2017-08-29 01:31:00 UTC
Description	Cross-site scripting (XSS) vulnerability in the Contact Save module 6.x-1.x before 6.x-1.5 for Drupal allows remote authentication

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	Steindom	Contact Save	6.x-1.0	All	All	All
Application	Steindom	Contact Save	6.x-1.1	All	All	All
Application	Steindom	Contact Save	6.x-1.1	beta1	All	All
Application	Steindom	Contact Save	6.x-1.2	All	All	All
Application	Steindom	Contact Save	6.x-1.2	beta1	All	All
Application	Steindom	Contact Save	6.x-1.2	beta2	All	All
Application	Steindom	Contact Save	6.x-1.2	beta3	All	All
Application	Steindom	Contact Save	6.x-1.3	All	All	All
Application	Steindom	Contact Save	6.x-1.3	beta1	All	All
Application	Steindom	Contact Save	6.x-1.3	beta2	All	All
Application	Steindom	Contact Save	6.x-1.3	beta3	All	All
Application	Steindom	Contact Save	6.x-1.4	All	All	All
Application	Steindom	Contact Save	6.x-1.4	beta1	All	All
Application	Steindom	Contact Save	6.x-1.4	beta2	All	All
Application	Steindom	Contact Save	6.x-1.5	All	All	All

Application	Steindom	Contact Save	6.x-1.x	dev	All	All
Application	Steindom	Contact Save	6.x-1.0	All	All	All
Application	Steindom	Contact Save	6.x-1.1	All	All	All
Application	Steindom	Contact Save	6.x-1.1	beta1	All	All
Application	Steindom	Contact Save	6.x-1.2	All	All	All
Application	Steindom	Contact Save	6.x-1.2	beta1	All	All
Application	Steindom	Contact Save	6.x-1.2	beta2	All	All
Application	Steindom	Contact Save	6.x-1.2	beta3	All	All
Application	Steindom	Contact Save	6.x-1.3	All	All	All
Application	Steindom	Contact Save	6.x-1.3	beta1	All	All
Application	Steindom	Contact Save	6.x-1.3	beta2	All	All
Application	Steindom	Contact Save	6.x-1.3	beta3	All	All
Application	Steindom	Contact Save	6.x-1.4	All	All	All
Application	Steindom	Contact Save	6.x-1.4	beta1	All	All
Application	Steindom	Contact Save	6.x-1.4	beta2	All	All
Application	Steindom	Contact Save	6.x-1.5	All	All	All
Application	Steindom	Contact Save	6.x-1.x	dev	All	All

References						
Reference				Source	Link	
Security Advisory SA48619 - Drupal Contact Save Module Unspecified Script Insertion Vulnerability - Secunia				SECUNIA	secunia.com	
80669				OSVDB	osvdb.org	
Log in Drupal.org				CONFIRM	drupalcode.org	
IBM X-Force Exchange				XF	exchange.xforce	
oss-security - CVE's for Drupal Contrib 2012 001 through 057 (67 new CVE assignments)				MLIST	www.openwall.c	
contact_save 6.x-1.5 drupal.org				CONFIRM	drupal.org	
Drupal Contact Save Module Unspecified Cross Site Scripting Vulnerability				BID	www.securityfo	
SA-CONTRIB-2012-048 - Contact Save - Cross Site Scripting drupal.org				MISC	drupal.org	
CVE Program record				CVE.ORG	www.cve.org	
NVD vulnerability detail				NVD	nvd.nist.gov	

No vendor comments have been submitted for this CVE.

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

© [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](#) and the authoritative source of CVE content is [MITRE's CVE web site](#). 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](#)