



# CVE-2009-3156

[MITRE](#)[NVD](#)[CVE.ORG](#)[JSON API](#)[Print: PDF !\[\]\(003082e50e3009141f59bd5df831749f\_img.jpg\)](#)

## Summary

<b>CVE</b>	CVE-2009-3156
<b>State</b>	PUBLISHED
<b>Assigner</b>	mitre
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2009-09-10 18:30:00 UTC
<b>Updated</b>	2026-04-23 00:35:47 UTC
<b>Description</b>	Cross-site scripting (XSS) vulnerability in the Date Tools sub-module in the Date module 6.x before 6.x-2.3 for Drupal allow

## Risk And Classification

**Primary CVSS:** v2.0 2.1 from nvd@nist.gov

AV:N/AC:H/Au:S/C:N/I:P/A:N

**Problem Types:** CWE-79 | n/a

## CVSS v2.0 Breakdown

Access Vector

Network

Access Complexity

High

Authentication

Single

Confidentiality

None

Integrity

Partial

Availability

None

AV:N/AC:H/Au:S/C:N/I:P/A:N

## NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Drupal	Drupal	All	All	All	All

Application	<a href="#">Karen Stevenson</a>	<a href="#">Date</a>	6.x-1.0-beta	All	All	All
Application	<a href="#">Karen Stevenson</a>	<a href="#">Date</a>	6.x-1.x-dev	All	All	All
Application	<a href="#">Karen Stevenson</a>	<a href="#">Date</a>	6.x-2.0	All	All	All
Application	<a href="#">Karen Stevenson</a>	<a href="#">Date</a>	6.x-2.0	rc1	All	All
Application	<a href="#">Karen Stevenson</a>	<a href="#">Date</a>	6.x-2.0	rc2	All	All
Application	<a href="#">Karen Stevenson</a>	<a href="#">Date</a>	6.x-2.0	rc3	All	All
Application	<a href="#">Karen Stevenson</a>	<a href="#">Date</a>	6.x-2.0	rc4	All	All
Application	<a href="#">Karen Stevenson</a>	<a href="#">Date</a>	6.x-2.0	rc5	All	All
Application	<a href="#">Karen Stevenson</a>	<a href="#">Date</a>	6.x-2.0	rc6	All	All
Application	<a href="#">Karen Stevenson</a>	<a href="#">Date</a>	6.x-2.0-beta	All	All	All
Application	<a href="#">Karen Stevenson</a>	<a href="#">Date</a>	6.x-2.0-beta2	All	All	All
Application	<a href="#">Karen Stevenson</a>	<a href="#">Date</a>	6.x-2.0-beta3	All	All	All
Application	<a href="#">Karen Stevenson</a>	<a href="#">Date</a>	6.x-2.0-beta4	All	All	All
Application	<a href="#">Karen Stevenson</a>	<a href="#">Date</a>	6.x-2.1	All	All	All
Application	<a href="#">Karen Stevenson</a>	<a href="#">Date</a>	6.x-2.2	All	All	All

#### Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	Na	N/a	affected n/a	Not specified

#### References

Reference	Source
Multiple Drupal Modules Date Wizard HTML Injection Vulnerability	af854a3a-2127-422b-91ae-
[SECURITY] Fedora 11 Update: drupal-date-6.x.2.3-0.fc11	af854a3a-2127-422b-91ae-
SA-CONTRIB-2009-046 - Date - Cross Site Scripting   drupal.org	af854a3a-2127-422b-91ae-
[SECURITY] Fedora 10 Update: drupal-date-6.x.2.3-0.fc10	af854a3a-2127-422b-91ae-
IBM X-Force Exchange	af854a3a-2127-422b-91ae-
date 6.x-2.3   drupal.org	af854a3a-2127-422b-91ae-
Webmail : Solution de messagerie professionnelle - OVHcloud- OVH	af854a3a-2127-422b-91ae-
Drupal 6 Date/Calendar XSS Vulnerability   Linux/Apache/MySQL/PHP Security	af854a3a-2127-422b-91ae-
Drupal Date Module Script Insertion Vulnerability - Secunia Advisories - Vulnerability Information - Secunia.com	af854a3a-2127-422b-91ae-
www.osvdb.org/56608	af854a3a-2127-422b-91ae-
CVE Program record	CVE.ORG
NVD vulnerability detail	NVD

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](#)