



CVE-2015-6665

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

Summary

CVE	CVE-2015-6665
State	PUBLISHED
Assigner	mitre
Source Priority	CVE Program / NVD first with legacy fallback
Published	2015-08-24 14:59:22 UTC
Updated	2026-05-06 22:30:45 UTC
Description	Cross-site scripting (XSS) vulnerability in the Ajax handler in Drupal 7.x before 7.39 and the Ctools module 6.x-1.x before 6

Risk And Classification

Primary CVSS: v2.0 4.3 from nvd@nist.gov

AV:N/AC:M/Au:N/C:N/I:P/A:N

Problem Types: CWE-79 | n/a

CVSS v2.0 Breakdown

Access Vector

Network

Access Complexity

Medium

Authentication

None

Confidentiality

None

Integrity

Partial

Availability

None

AV:N/AC:M/Au:N/C:N/I:P/A:N

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Chaos Tool Suite Project	Ctools	6.x-1.0	All	All	All

Application	Chaos Tool Suite Project	Ctools	6.x-1.0	alpha1	All	All
Application	Chaos Tool Suite Project	Ctools	6.x-1.0	alpha2	All	All
Application	Chaos Tool Suite Project	Ctools	6.x-1.0	alpha3	All	All
Application	Chaos Tool Suite Project	Ctools	6.x-1.0	beta1	All	All
Application	Chaos Tool Suite Project	Ctools	6.x-1.0	beta2	All	All
Application	Chaos Tool Suite Project	Ctools	6.x-1.0	beta3	All	All
Application	Chaos Tool Suite Project	Ctools	6.x-1.0	beta4	All	All
Application	Chaos Tool Suite Project	Ctools	6.x-1.0	rc1	All	All
Application	Chaos Tool Suite Project	Ctools	6.x-1.1	All	All	All
Application	Chaos Tool Suite Project	Ctools	6.x-1.11	All	All	All
Application	Chaos Tool Suite Project	Ctools	6.x-1.12	All	All	All
Application	Chaos Tool Suite Project	Ctools	6.x-1.13	All	All	All
Application	Chaos Tool Suite Project	Ctools	6.x-1.2	All	All	All
Application	Chaos Tool Suite Project	Ctools	6.x-1.3	All	All	All
Application	Chaos Tool Suite Project	Ctools	6.x-1.4	All	All	All
Application	Chaos Tool Suite Project	Ctools	6.x-1.5	All	All	All
Application	Chaos Tool Suite Project	Ctools	6.x-1.6	All	All	All
Application	Chaos Tool Suite Project	Ctools	6.x-1.7	All	All	All
Application	Chaos Tool Suite Project	Ctools	6.x-1.8	All	All	All
Application	Chaos Tool Suite Project	Ctools	6.x-1.9	All	All	All
Application	Chaos Tool Suite Project	Ctools	6.x-1.x	dev	All	All
Application	Drupal	Drupal	7.0	All	All	All
Application	Drupal	Drupal	7.0	alpha1	All	All
Application	Drupal	Drupal	7.0	alpha2	All	All
Application	Drupal	Drupal	7.0	alpha3	All	All
Application	Drupal	Drupal	7.0	alpha4	All	All
Application	Drupal	Drupal	7.0	alpha5	All	All
Application	Drupal	Drupal	7.0	alpha6	All	All
Application	Drupal	Drupal	7.0	alpha7	All	All
Application	Drupal	Drupal	7.0	beta1	All	All
Application	Drupal	Drupal	7.0	beta2	All	All
Application	Drupal	Drupal	7.0	beta3	All	All
Application	Drupal	Drupal	7.0	dev	All	All
Application	Drupal	Drupal	7.0	rc1	All	All
Application	Drupal	Drupal	7.0	rc2	All	All
Application	Drupal	Drupal	7.0	rc3	All	All

Application	Drupal	Drupal	7.0	rc4	All	All
Application	Drupal	Drupal	7.1	All	All	All
Application	Drupal	Drupal	7.10	All	All	All
Application	Drupal	Drupal	7.11	All	All	All
Application	Drupal	Drupal	7.12	All	All	All
Application	Drupal	Drupal	7.13	All	All	All
Application	Drupal	Drupal	7.14	All	All	All
Application	Drupal	Drupal	7.15	All	All	All
Application	Drupal	Drupal	7.16	All	All	All
Application	Drupal	Drupal	7.17	All	All	All
Application	Drupal	Drupal	7.18	All	All	All
Application	Drupal	Drupal	7.19	All	All	All
Application	Drupal	Drupal	7.2	All	All	All
Application	Drupal	Drupal	7.20	All	All	All
Application	Drupal	Drupal	7.21	All	All	All
Application	Drupal	Drupal	7.22	All	All	All
Application	Drupal	Drupal	7.23	All	All	All
Application	Drupal	Drupal	7.24	All	All	All
Application	Drupal	Drupal	7.25	All	All	All
Application	Drupal	Drupal	7.26	All	All	All
Application	Drupal	Drupal	7.27	All	All	All
Application	Drupal	Drupal	7.28	All	All	All
Application	Drupal	Drupal	7.29	All	All	All
Application	Drupal	Drupal	7.3	All	All	All
Application	Drupal	Drupal	7.30	All	All	All
Application	Drupal	Drupal	7.33	All	All	All
Application	Drupal	Drupal	7.34	All	All	All
Application	Drupal	Drupal	7.35	All	All	All
Application	Drupal	Drupal	7.36	All	All	All
Application	Drupal	Drupal	7.37	All	All	All
Application	Drupal	Drupal	7.38	All	All	All
Application	Drupal	Drupal	7.4	All	All	All
Application	Drupal	Drupal	7.5	All	All	All
Application	Drupal	Drupal	7.6	All	All	All
Application	Drupal	Drupal	7.7	All	All	All

Application	Drupal	Drupal	7.8	All	All	All
Application	Drupal	Drupal	7.9	All	All	All
Application	Drupal	Drupal	7.x-dev	All	All	All
Operating System	Fedoraproject	Fedora	21	All	All	All
Operating System	Fedoraproject	Fedora	22	All	All	All
Operating System	Fedoraproject	Fedora	23	All	All	All

Vendor Declared Affected Products

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

References

Reference
[SECURITY] Fedora 22 Update: drupal6-6.37-1.fc22
[SECURITY] Fedora 23 Update: drupal6-6.37-1.fc23
[SECURITY] Fedora 21 Update: drupal6-ctools-1.14-1.fc21
[SECURITY] Fedora 22 Update: drupal7-7.39-1.fc22
Drupal Ajax System Cross Site Scripting Vulnerability
[SECURITY] Fedora 22 Update: drupal6-ctools-1.14-1.fc22
Drupal Multiple Flaws Let Remote Users Conduct Cross-Site Scripting and Cross-Site Request Forgery Attacks and Remote Authenticated Us
Drupal Core - Critical - Multiple Vulnerabilities - SA-CORE-2015-003 Drupal.org
[SECURITY] Fedora 23 Update: drupal6-ctools-1.14-1.fc23
[SECURITY] Fedora 21 Update: drupal6-6.37-1.fc21
[SECURITY] Fedora 21 Update: drupal7-7.39-1.fc21
Debian -- Security Information -- DSA-3346-1 drupal7
Ctools - Critical - Multiple Vulnerabilities - SA-CONTRIB-2015-141 Drupal.org
ctools 6.x-1.14 Drupal.org
[SECURITY] Fedora 23 Update: drupal7-7.39-1.fc23
CVE Program record
NVD vulnerability detail

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](#)