



CVE-2016-7140

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

Summary

CVE	CVE-2016-7140
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2017-03-07 16:59:00 UTC
Updated	2018-10-09 20:00:00 UTC
Description	Multiple cross-site scripting (XSS) vulnerabilities in the ZMI page in Zope2 in Plone CMS 5.x through 5.0.6, 4.x through 4.3.

Risk And Classification

Problem Types: CWE-79

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Plone	Plone	3.3	All	All	All
Application	Plone	Plone	3.3.1	All	All	All
Application	Plone	Plone	3.3.2	All	All	All
Application	Plone	Plone	3.3.3	All	All	All
Application	Plone	Plone	3.3.4	All	All	All
Application	Plone	Plone	3.3.5	All	All	All
Application	Plone	Plone	3.3.6	All	All	All
Application	Plone	Plone	4.0	All	All	All
Application	Plone	Plone	4.0.1	All	All	All
Application	Plone	Plone	4.0.10	All	All	All
Application	Plone	Plone	4.0.2	All	All	All
Application	Plone	Plone	4.0.3	All	All	All
Application	Plone	Plone	4.0.4	All	All	All
Application	Plone	Plone	4.0.5	All	All	All
Application	Plone	Plone	4.0.7	All	All	All
Application	Plone	Plone	4.0.8	All	All	All
Application	Plone	Plone	4.0.9	All	All	All

Application	Plone	Plone	4.1	All	All	All
Application	Plone	Plone	4.1.1	All	All	All
Application	Plone	Plone	4.1.2	All	All	All
Application	Plone	Plone	4.1.3	All	All	All
Application	Plone	Plone	4.1.4	All	All	All
Application	Plone	Plone	4.1.5	All	All	All
Application	Plone	Plone	4.1.6	All	All	All
Application	Plone	Plone	4.2	All	All	All
Application	Plone	Plone	4.2.1	All	All	All
Application	Plone	Plone	4.2.2	All	All	All
Application	Plone	Plone	4.2.3	All	All	All
Application	Plone	Plone	4.2.4	All	All	All
Application	Plone	Plone	4.2.5	All	All	All
Application	Plone	Plone	4.2.6	All	All	All
Application	Plone	Plone	4.2.7	All	All	All
Application	Plone	Plone	4.3	All	All	All
Application	Plone	Plone	4.3.1	All	All	All
Application	Plone	Plone	4.3.10	All	All	All
Application	Plone	Plone	4.3.11	All	All	All
Application	Plone	Plone	4.3.2	All	All	All
Application	Plone	Plone	4.3.3	All	All	All
Application	Plone	Plone	4.3.4	All	All	All
Application	Plone	Plone	4.3.5	All	All	All
Application	Plone	Plone	4.3.6	All	All	All
Application	Plone	Plone	4.3.7	All	All	All
Application	Plone	Plone	4.3.8	All	All	All
Application	Plone	Plone	4.3.9	All	All	All
Application	Plone	Plone	5.0	All	All	All
Application	Plone	Plone	5.0	a1	All	All
Application	Plone	Plone	5.0	rc1	All	All
Application	Plone	Plone	5.0	rc2	All	All
Application	Plone	Plone	5.0	rc3	All	All
Application	Plone	Plone	5.0.1	All	All	All
Application	Plone	Plone	5.0.2	All	All	All
Application	Plone	Plone	5.0.3	All	All	All

Application	Plone	Plone	5.0.4	All	All	All
Application	Plone	Plone	5.0.5	All	All	All
Application	Plone	Plone	5.0.6	All	All	All
Application	Plone	Plone	5.1a1	All	All	All
Application	Plone	Plone	3.3	All	All	All
Application	Plone	Plone	3.3.1	All	All	All
Application	Plone	Plone	3.3.2	All	All	All
Application	Plone	Plone	3.3.3	All	All	All
Application	Plone	Plone	3.3.4	All	All	All
Application	Plone	Plone	3.3.5	All	All	All
Application	Plone	Plone	3.3.6	All	All	All
Application	Plone	Plone	4.0	All	All	All
Application	Plone	Plone	4.0.1	All	All	All
Application	Plone	Plone	4.0.10	All	All	All
Application	Plone	Plone	4.0.2	All	All	All
Application	Plone	Plone	4.0.3	All	All	All
Application	Plone	Plone	4.0.4	All	All	All
Application	Plone	Plone	4.0.5	All	All	All
Application	Plone	Plone	4.0.7	All	All	All
Application	Plone	Plone	4.0.8	All	All	All
Application	Plone	Plone	4.0.9	All	All	All
Application	Plone	Plone	4.1	All	All	All
Application	Plone	Plone	4.1.1	All	All	All
Application	Plone	Plone	4.1.2	All	All	All
Application	Plone	Plone	4.1.3	All	All	All
Application	Plone	Plone	4.1.4	All	All	All
Application	Plone	Plone	4.1.5	All	All	All
Application	Plone	Plone	4.1.6	All	All	All
Application	Plone	Plone	4.2	All	All	All
Application	Plone	Plone	4.2.1	All	All	All
Application	Plone	Plone	4.2.2	All	All	All
Application	Plone	Plone	4.2.3	All	All	All
Application	Plone	Plone	4.2.4	All	All	All
Application	Plone	Plone	4.2.5	All	All	All
Application	Plone	Plone	4.2.6	All	All	All
Application	Plone	Plone	4.2.7	All	All	All

Application	Plone	Plone	4.2.7	All	All	All
Application	Plone	Plone	4.3	All	All	All
Application	Plone	Plone	4.3.1	All	All	All
Application	Plone	Plone	4.3.10	All	All	All
Application	Plone	Plone	4.3.11	All	All	All
Application	Plone	Plone	4.3.2	All	All	All
Application	Plone	Plone	4.3.3	All	All	All
Application	Plone	Plone	4.3.4	All	All	All
Application	Plone	Plone	4.3.5	All	All	All
Application	Plone	Plone	4.3.6	All	All	All
Application	Plone	Plone	4.3.7	All	All	All
Application	Plone	Plone	4.3.8	All	All	All
Application	Plone	Plone	4.3.9	All	All	All
Application	Plone	Plone	5.0	All	All	All
Application	Plone	Plone	5.0	a1	All	All
Application	Plone	Plone	5.0	rc1	All	All
Application	Plone	Plone	5.0	rc2	All	All
Application	Plone	Plone	5.0	rc3	All	All
Application	Plone	Plone	5.0.1	All	All	All
Application	Plone	Plone	5.0.2	All	All	All
Application	Plone	Plone	5.0.3	All	All	All
Application	Plone	Plone	5.0.4	All	All	All
Application	Plone	Plone	5.0.5	All	All	All
Application	Plone	Plone	5.0.6	All	All	All
Application	Plone	Plone	5.1a1	All	All	All

References						
Reference			Source	Link	Tags	
Full Disclosure: Multiple Vulnerabilities in Plone CMS			FULLDISC	seclists.org	Third Party Advisory	
Non-Persistent XSS in Zope2 — Plone.org			CONFIRM	plone.org	Vendor Advisory	
SecurityFocus			BUGTRAQ	www.securityfocus.com		
oss-security - Re: CVE request: Plone multiple vulnerabilities			MLIST	www.openwall.com	Mailing List, Patch, ...	
oss-security - Re: CVE request: Plone multiple vulnerabilities			MLIST	www.openwall.com	Mailing List, Patch, ...	
Plone Multiple Security vulnerabilities			BID	www.securityfocus.com		
Plone CMS 4.3.11 / 5.0.6 XSS / Traversal / Open Redirection ≈ Packet Storm			MISC	packetstormsecurity.com	Exploit, Third Party ...	
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