CVE-2009-5145

MITRE | NVD | CVE.ORG | JSON API | Print: PDF

Summary

CVE	CVE-2009-5145
State	PUBLIC
Assigner	secalert@redhat.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2017-08-07 17:29:00 UTC
Updated	2017-08-15 16:29:00 UTC
Description	Cross-site scripting (XSS) vulnerability in ZMI pages that use the manage_tabs_message in Zope 2.11.4, 2.11.2, 2.10.9, 2.

Risk And Classification

Problem Types: CWE-79

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Zope	Zope	2.10.1	All	All	All
Application	Zope	Zope	2.10.2	All	All	All
Application	Zope	Zope	2.10.4	All	All	All
Application	Zope	Zope	2.10.5	All	All	All
Application	Zope	Zope	2.10.6	All	All	All
Application	Zope	Zope	2.10.7	All	All	All
Application	Zope	Zope	2.10.9	All	All	All
Application	Zope	Zope	2.11.2	All	All	All
Application	Zope	Zope	2.11.4	All	All	All
Application	Zope	Zope	2.12.0	All	All	All
Application	Zope	Zope	2.10.1	All	All	All
Application	Zope	Zope	2.10.2	All	All	All
Application	Zope	Zope	2.10.4	All	All	All
Application	Zope	Zope	2.10.5	All	All	All
Application	Zope	Zope	2.10.6	All	All	All
Application	Zope	Zope	2.10.7	All	All	All
Application	Zope	Zope	2.10.9	All	All	All

Application	Zope	Zope	2.11.2	All	All	All
Application	Zope	Zope	2.11.4	All	All	All
Application	Zope	Zope	2.12.0	All	All	All

References

Reference	Source	Link
LP #490514: preserve tainting when calling into DTML from ZPT. · zopefoundation/Zope@2abdf14 · GitHub	CONFIRM	github.com
Bug #490514 “XSS Vulnerability in ZMI” : Bugs : Zope 2	CONFIRM	bugs.launchpad.ne
oss-security - Re: XSS In Zope	MLIST	www.openwall.com
CVE-2009-5145	MISC	security-tracker.de
Zope 'manage_tabs_message' Parameter Cross Site Scripting Vulnerability	BID	www.securityfocus
** RESERVED ** · CVE-2009-5145	MISC	cve.killedkenny.io
Zope 'manage_tabs_message' Parameter Cross Site Scripting Vulnerability	MITRE	www.securityfocus
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.