CVE-2013-5320

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

Summary

CVE	CVE-2013-5320
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2013-08-20 14:55:00 UTC
Updated	2017-08-29 01:33:00 UTC
Description	Cross-site scripting (XSS) vulnerability in Forums/EditPost.aspx in mojoPortal before 2.3.9.8 allows remote attackers to inje

Risk And Classification

Problem Types: CWE-79

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Sourcetreesolutions	Mojoportal	2.3.0.1	All	All	All
Application	Sourcetreesolutions	Mojoportal	2.3.0.4	All	All	All
Application	Sourcetreesolutions	Mojoportal	2.3.0.8	All	All	All
Application	Sourcetreesolutions	Mojoportal	2.3.1.0	All	All	All
Application	Sourcetreesolutions	Mojoportal	2.3.1.3	All	All	All
Application	Sourcetreesolutions	Mojoportal	2.3.1.5	All	All	All
Application	Sourcetreesolutions	Mojoportal	2.3.1.6	All	All	All
Application	Sourcetreesolutions	Mojoportal	2.3.1.7	All	All	All
Application	Sourcetreesolutions	Mojoportal	2.3.1.9	All	All	All
Application	Sourcetreesolutions	Mojoportal	2.3.2.9	All	All	All
Application	Sourcetreesolutions	Mojoportal	2.3.3.2	All	All	All
Application	Sourcetreesolutions	Mojoportal	2.3.3.4	All	All	All
Application	Sourcetreesolutions	Mojoportal	2.3.3.6	All	All	All
Application	Sourcetreesolutions	Mojoportal	2.3.3.9	All	All	All
Application	Sourcetreesolutions	Mojoportal	2.3.4.1	All	All	All
Application	Sourcetreesolutions	Mojoportal	2.3.4.2	All	All	All
Application	Sourcetreesolutions	Mojoportal	2.3.4.4	All	All	All

Application	Sourcetreesolutions	Mojoportal	2.3.4.5	All	All	All
Application	Sourcetreesolutions	Mojoportal	2.3.4.8	All	All	All
Application	Sourcetreesolutions	Mojoportal	2.3.5.2	All	All	All
Application	Sourcetreesolutions	Mojoportal	2.3.5.3	All	All	All
Application	Sourcetreesolutions	Mojoportal	2.3.5.4	All	All	All
Application	Sourcetreesolutions	Mojoportal	2.3.5.5	All	All	All
Application	Sourcetreesolutions	Mojoportal	2.3.5.8	All	All	All
Application	Sourcetreesolutions	Mojoportal	2.3.6.1	All	All	All
Application	Sourcetreesolutions	Mojoportal	2.3.6.2	All	All	All
Application	Sourcetreesolutions	Mojoportal	2.3.6.4	All	All	All
Application	Sourcetreesolutions	Mojoportal	2.3.6.5	All	All	All
Application	Sourcetreesolutions	Mojoportal	2.3.6.6	All	All	All
Application	Sourcetreesolutions	Mojoportal	2.3.6.7	All	All	All
Application	Sourcetreesolutions	Mojoportal	2.3.7.5	All	All	All
Application	Sourcetreesolutions	Mojoportal	2.3.7.6	All	All	All
Application	Sourcetreesolutions	Mojoportal	2.3.8.1	All	All	All
Application	Sourcetreesolutions	Mojoportal	2.3.8.5	All	All	All
Application	Sourcetreesolutions	Mojoportal	2.3.9.0	All	All	All
Application	Sourcetreesolutions	Mojoportal	2.3.9.3	All	All	All
Application	Sourcetreesolutions	Mojoportal	2.3.9.4	All	All	All
Application	Sourcetreesolutions	Mojoportal	2.3.9.5	All	All	All
Application	Sourcetreesolutions	Mojoportal	2.3.9.6	All	All	All
Application	Sourcetreesolutions	Mojoportal	2.3.0.1	All	All	All
Application	Sourcetreesolutions	Mojoportal	2.3.0.4	All	All	All
Application	Sourcetreesolutions	Mojoportal	2.3.0.8	All	All	All
Application	Sourcetreesolutions	Mojoportal	2.3.1.0	All	All	All
Application	Sourcetreesolutions	Mojoportal	2.3.1.3	All	All	All
Application	Sourcetreesolutions	Mojoportal	2.3.1.5	All	All	All
Application	Sourcetreesolutions	Mojoportal	2.3.1.6	All	All	All
Application	Sourcetreesolutions	Mojoportal	2.3.1.7	All	All	All
Application	Sourcetreesolutions	Mojoportal	2.3.1.9	All	All	All
Application	Sourcetreesolutions	Mojoportal	2.3.2.9	All	All	All
Application	Sourcetreesolutions	Mojoportal	2.3.3.2	All	All	All
Application	Sourcetreesolutions	Mojoportal	2.3.3.4	All	All	All
Application	Sourcetreesolutions	Mojoportal	2.3.3.6	All	All	All

Application	Sourcetreesolutions	Mojoportal	2.3.3.9	All	All	All
Application	Sourcetreesolutions	Mojoportal	2.3.4.1	All	All	All
Application	Sourcetreesolutions	Mojoportal	2.3.4.2	All	All	All
Application	Sourcetreesolutions	Mojoportal	2.3.4.4	All	All	All
Application	Sourcetreesolutions	Mojoportal	2.3.4.5	All	All	All
Application	Sourcetreesolutions	Mojoportal	2.3.4.8	All	All	All
Application	Sourcetreesolutions	Mojoportal	2.3.5.2	All	All	All
Application	Sourcetreesolutions	Mojoportal	2.3.5.3	All	All	All
Application	Sourcetreesolutions	Mojoportal	2.3.5.4	All	All	All
Application	Sourcetreesolutions	Mojoportal	2.3.5.5	All	All	All
Application	Sourcetreesolutions	Mojoportal	2.3.5.8	All	All	All
Application	Sourcetreesolutions	Mojoportal	2.3.6.1	All	All	All
Application	Sourcetreesolutions	Mojoportal	2.3.6.2	All	All	All
Application	Sourcetreesolutions	Mojoportal	2.3.6.4	All	All	All
Application	Sourcetreesolutions	Mojoportal	2.3.6.5	All	All	All
Application	Sourcetreesolutions	Mojoportal	2.3.6.6	All	All	All
Application	Sourcetreesolutions	Mojoportal	2.3.6.7	All	All	All
Application	Sourcetreesolutions	Mojoportal	2.3.7.5	All	All	All
Application	Sourcetreesolutions	Mojoportal	2.3.7.6	All	All	All
Application	Sourcetreesolutions	Mojoportal	2.3.8.1	All	All	All
Application	Sourcetreesolutions	Mojoportal	2.3.8.5	All	All	All
Application	Sourcetreesolutions	Mojoportal	2.3.9.0	All	All	All
Application	Sourcetreesolutions	Mojoportal	2.3.9.3	All	All	All
Application	Sourcetreesolutions	Mojoportal	2.3.9.4	All	All	All
Application	Sourcetreesolutions	Mojoportal	2.3.9.5	All	All	All
Application	Sourcetreesolutions	Mojoportal	2.3.9.6	All	All	All
Application	Sourcetreesolutions	Mojoportal	All	All	All	All

References

Reference	Source	Link
mojoportal HTML Injection Vulnerability	BID	www.securityfocus.co
MojoPortal 2.3.9.7 Cross Site Scripting ≈ Packet Storm	MISC	packetstormsecurity.c
mojoPortal 2.3.9.8 Released - mojoPortal	CONFIRM	www.mojoportal.com
Security Advisory SA54297 - mojoPortal "txtSubject" Script Insertion Vulnerability - Secunia	SECUNIA	secunia.com
95847	OSVDB	osvdb.org
20130730 MojoPortal XSS	BUGTRAQ	archives.neohapsis.cc

IBM X-Force Exchange	XF	exchange.xforce.ibmc
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.