



CVE-2010-2123

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

Summary

CVE	CVE-2010-2123
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2010-06-01 21:30:00 UTC
Updated	2017-08-17 01:32:00 UTC
Description	Multiple cross-site scripting (XSS) vulnerabilities in the Storm module 5.x and 6.x before 6.x-1.33 for Drupal allow remote au

Risk And Classification

Problem Types: CWE-79

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Drupal	Drupal	All	All	All	All
Application	Drupal	Drupal	All	All	All	All
Application	Speedtech	Storm	5.x-1.1	All	All	All
Application	Speedtech	Storm	5.x-1.10	All	All	All
Application	Speedtech	Storm	5.x-1.11	All	All	All
Application	Speedtech	Storm	5.x-1.12	All	All	All
Application	Speedtech	Storm	5.x-1.13	All	All	All
Application	Speedtech	Storm	5.x-1.14	All	All	All
Application	Speedtech	Storm	5.x-1.2	All	All	All
Application	Speedtech	Storm	5.x-1.3	All	All	All
Application	Speedtech	Storm	5.x-1.4	All	All	All
Application	Speedtech	Storm	5.x-1.5	All	All	All
Application	Speedtech	Storm	5.x-1.6	All	All	All
Application	Speedtech	Storm	5.x-1.7	All	All	All
Application	Speedtech	Storm	5.x-1.8	All	All	All
Application	Speedtech	Storm	5.x-1.9	All	All	All
Application	Speedtech	Storm	5.x-1.x	dev	All	All

Application	Speedtech	Storm	6.x-1.0	All	All	All
Application	Speedtech	Storm	6.x-1.1	All	All	All
Application	Speedtech	Storm	6.x-1.10	All	All	All
Application	Speedtech	Storm	6.x-1.11	All	All	All
Application	Speedtech	Storm	6.x-1.12	All	All	All
Application	Speedtech	Storm	6.x-1.13	All	All	All
Application	Speedtech	Storm	6.x-1.14	All	All	All
Application	Speedtech	Storm	6.x-1.15	All	All	All
Application	Speedtech	Storm	6.x-1.16	All	All	All
Application	Speedtech	Storm	6.x-1.17	All	All	All
Application	Speedtech	Storm	6.x-1.18	All	All	All
Application	Speedtech	Storm	6.x-1.19	All	All	All
Application	Speedtech	Storm	6.x-1.2	All	All	All
Application	Speedtech	Storm	6.x-1.20	All	All	All
Application	Speedtech	Storm	6.x-1.21	All	All	All
Application	Speedtech	Storm	6.x-1.22	All	All	All
Application	Speedtech	Storm	6.x-1.23	All	All	All
Application	Speedtech	Storm	6.x-1.24	All	All	All
Application	Speedtech	Storm	6.x-1.25	All	All	All
Application	Speedtech	Storm	6.x-1.26	All	All	All
Application	Speedtech	Storm	6.x-1.27	All	All	All
Application	Speedtech	Storm	6.x-1.28	All	All	All
Application	Speedtech	Storm	6.x-1.29	All	All	All
Application	Speedtech	Storm	6.x-1.3	All	All	All
Application	Speedtech	Storm	6.x-1.30	All	All	All
Application	Speedtech	Storm	6.x-1.31	All	All	All
Application	Speedtech	Storm	6.x-1.32	All	All	All
Application	Speedtech	Storm	6.x-1.4	All	All	All
Application	Speedtech	Storm	6.x-1.5	All	All	All
Application	Speedtech	Storm	6.x-1.6	All	All	All
Application	Speedtech	Storm	6.x-1.7	All	All	All
Application	Speedtech	Storm	6.x-1.8	All	All	All
Application	Speedtech	Storm	6.x-1.9	All	All	All
Application	Speedtech	Storm	6.x-1.x	dev	All	All
Application	Speedtech	Storm	5.x-1.1	All	All	All

Application	Speedtech	Storm	5.x-1.10	All	All	All
Application	Speedtech	Storm	5.x-1.11	All	All	All
Application	Speedtech	Storm	5.x-1.12	All	All	All
Application	Speedtech	Storm	5.x-1.13	All	All	All
Application	Speedtech	Storm	5.x-1.14	All	All	All
Application	Speedtech	Storm	5.x-1.2	All	All	All
Application	Speedtech	Storm	5.x-1.3	All	All	All
Application	Speedtech	Storm	5.x-1.4	All	All	All
Application	Speedtech	Storm	5.x-1.5	All	All	All
Application	Speedtech	Storm	5.x-1.6	All	All	All
Application	Speedtech	Storm	5.x-1.7	All	All	All
Application	Speedtech	Storm	5.x-1.8	All	All	All
Application	Speedtech	Storm	5.x-1.9	All	All	All
Application	Speedtech	Storm	5.x-1.x	dev	All	All
Application	Speedtech	Storm	6.x-1.0	All	All	All
Application	Speedtech	Storm	6.x-1.1	All	All	All
Application	Speedtech	Storm	6.x-1.10	All	All	All
Application	Speedtech	Storm	6.x-1.11	All	All	All
Application	Speedtech	Storm	6.x-1.12	All	All	All
Application	Speedtech	Storm	6.x-1.13	All	All	All
Application	Speedtech	Storm	6.x-1.14	All	All	All
Application	Speedtech	Storm	6.x-1.15	All	All	All
Application	Speedtech	Storm	6.x-1.16	All	All	All
Application	Speedtech	Storm	6.x-1.17	All	All	All
Application	Speedtech	Storm	6.x-1.18	All	All	All
Application	Speedtech	Storm	6.x-1.19	All	All	All
Application	Speedtech	Storm	6.x-1.2	All	All	All
Application	Speedtech	Storm	6.x-1.20	All	All	All
Application	Speedtech	Storm	6.x-1.21	All	All	All
Application	Speedtech	Storm	6.x-1.22	All	All	All
Application	Speedtech	Storm	6.x-1.23	All	All	All
Application	Speedtech	Storm	6.x-1.24	All	All	All
Application	Speedtech	Storm	6.x-1.25	All	All	All
Application	Speedtech	Storm	6.x-1.26	All	All	All
Application	Speedtech	Storm	6.x-1.27	All	All	All
Application	Speedtech	Storm	6.x-1.28	All	All	All

Application	Speedtech	Storm	6.x-1.28	All	All	All
Application	Speedtech	Storm	6.x-1.29	All	All	All
Application	Speedtech	Storm	6.x-1.3	All	All	All
Application	Speedtech	Storm	6.x-1.30	All	All	All
Application	Speedtech	Storm	6.x-1.31	All	All	All
Application	Speedtech	Storm	6.x-1.32	All	All	All
Application	Speedtech	Storm	6.x-1.4	All	All	All
Application	Speedtech	Storm	6.x-1.5	All	All	All
Application	Speedtech	Storm	6.x-1.6	All	All	All
Application	Speedtech	Storm	6.x-1.7	All	All	All
Application	Speedtech	Storm	6.x-1.8	All	All	All
Application	Speedtech	Storm	6.x-1.9	All	All	All
Application	Speedtech	Storm	6.x-1.x	dev	All	All

References			
Reference	Source	Link	Tags
IBM X-Force Exchange	XF	exchange.xforce.ibmcloud.com	
SA-CONTRIB-2010-054 - Storm - Cross Site Scripting (XSS) drupal.org	CONFIRM	drupal.org	Patch
64616	OSVDB	www.osvdb.org	
NEOHAPSIS - Peace of Mind Through Integrity and Insight	FULLDISC	archives.neohapsis.com	Explo
Drupal Storm Project HTML Injection Vulnerability	BID	www.securityfocus.com	Patch
Drupal Storm Module Multiple Script Insertion Vulnerabilities - Advisories - Community	SECUNIA	secunia.com	Vend
CVE Program record	CVE.ORG	www.cve.org	canon
NVD vulnerability detail	NVD	nvd.nist.gov	canon

No vendor comments have been submitted for this CVE.

There are currently no legacy QID mappings associated with this CVE.