CVE-2011-5226

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

Summary

CVE	CVE-2011-5226
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2012-10-25 17:55:00 UTC
Updated	2023-11-07 02:09:00 UTC
Description	Cross-site request forgery (CSRF) vulnerability in wordpress_sentinel.php in the Sentinel plugin 1.0.0 for WordPress allows

Risk And Classification

Problem Types: CWE-352

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Trioniclabs	Sentinel	1.0.0	All	All	All
Application	Trioniclabs	Sentinel	1.0.0	All	All	All
Application	Wordpress	Wordpress	-	All	All	All
Application	Wordpress	Wordpress	-	All	All	All

References

Reference	Source	Link
403 Forbidden		plugins.t
403 Forbidden	CONFIRM	plugins.t
WordPress › WordPress Sentinel « WordPress Plugins	CONFIRM	wordpres
77778	OSVDB	osvdb.or
IBM X-Force Exchange	XF	exchang
Sentinel Plugin for WordPress Cross Site Scripting and Cross Site Request Forgery Vulnerabilities	BID	www.sec
About Secunia Research | Flexera	SECUNIA	secunia.c
Le plugin "WordPress Sentinel" 1.0.1 contient des failles de sécurité de type XSS, CSRF et SQLi » blog.boiteaweb.fr	MISC	www.boi
CVE Program record	CVE.ORG	www.cve
NVD vulnerability detail	NVD	nvd.nist.g

No vendor comments have been submitted for this CVE.

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

Free CVE JSON API cve.report/api

CVE.report and Source URL Uptime Status **status.cve.report**