



CVE-2014-4030

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

Summary

CVE	CVE-2014-4030
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2014-06-25 20:55:00 UTC
Updated	2014-06-26 14:25:00 UTC
Description	Cross-site request forgery (CSRF) vulnerability in the JW Player plugin before 2.1.4 for WordPress allows remote attackers

Risk And Classification

Problem Types: CWE-352

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Longtailvideo	Jw Player For Flash Html5 Video Plugin	2.0.0	All	All	All
Application	Longtailvideo	Jw Player For Flash Html5 Video Plugin	2.0.1	All	All	All
Application	Longtailvideo	Jw Player For Flash Html5 Video Plugin	2.0.2	All	All	All
Application	Longtailvideo	Jw Player For Flash Html5 Video Plugin	2.0.3	All	All	All
Application	Longtailvideo	Jw Player For Flash Html5 Video Plugin	2.0.4	All	All	All
Application	Longtailvideo	Jw Player For Flash Html5 Video Plugin	2.0.5	All	All	All
Application	Longtailvideo	Jw Player For Flash Html5 Video Plugin	2.1.0	All	All	All
Application	Longtailvideo	Jw Player For Flash Html5 Video Plugin	2.1.1	All	All	All
Application	Longtailvideo	Jw Player For Flash Html5 Video Plugin	2.1.2	All	All	All
Application	Longtailvideo	Jw Player For Flash Html5 Video Plugin	All	All	All	All
Application	Longtailvideo	Jw Player For Flash Html5 Video Plugin	2.0.0	All	All	All
Application	Longtailvideo	Jw Player For Flash Html5 Video Plugin	2.0.1	All	All	All
Application	Longtailvideo	Jw Player For Flash Html5 Video Plugin	2.0.2	All	All	All
Application	Longtailvideo	Jw Player For Flash Html5 Video Plugin	2.0.3	All	All	All
Application	Longtailvideo	Jw Player For Flash Html5 Video Plugin	2.0.4	All	All	All
Application	Longtailvideo	Jw Player For Flash Html5 Video Plugin	2.0.5	All	All	All
Application	Longtailvideo	Jw Player For Flash Html5 Video Plugin	2.1.0	All	All	All

Application	Longtailvideo	Jw Player For Flash Html5 Video Plugin	2.1.1	All	All	All
Application	Longtailvideo	Jw Player For Flash Html5 Video Plugin	2.1.2	All	All	All
Application	Longtailvideo	Jw Player For Flash Html5 Video Plugin	2.0.0	All	All	All
Application	Longtailvideo	Jw Player For Flash Html5 Video Plugin	2.0.1	All	All	All
Application	Longtailvideo	Jw Player For Flash Html5 Video Plugin	2.0.2	All	All	All
Application	Longtailvideo	Jw Player For Flash Html5 Video Plugin	2.0.3	All	All	All
Application	Longtailvideo	Jw Player For Flash Html5 Video Plugin	2.0.4	All	All	All
Application	Longtailvideo	Jw Player For Flash Html5 Video Plugin	2.0.5	All	All	All
Application	Longtailvideo	Jw Player For Flash Html5 Video Plugin	2.1.0	All	All	All
Application	Longtailvideo	Jw Player For Flash Html5 Video Plugin	2.1.1	All	All	All
Application	Longtailvideo	Jw Player For Flash Html5 Video Plugin	2.1.2	All	All	All
Application	Longtailvideo	Jw Player For Flash Html5 Video Plugin	All	All	All	All

References

Reference	Source	Link
WordPress › JW Player for Flash & HTML5 Video « WordPress Plugins	CONFIRM	wordpress.
Full Disclosure: CSRF in JW Player for Flash & HTML5 Video 2.1.2 permits deletion of players (WordPress plugin)	FULLDISC	seclists.org
CSRF in JW Player for Flash & HTML5 Video 2.1.3 permits deletion of players dxwsecurity	MISC	security.dx
Security Advisory SA59173 - WordPress JW Player Plugin Cross-Site Request Forgery Vulnerability - Secunia	SECUNIA	secunia.co
CVE Program record	CVE.ORG	www.cve.o
NVD vulnerability detail	NVD	nvd.nist.go

No vendor comments have been submitted for this CVE.

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