



CVE-2012-4915

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

Summary

CVE	CVE-2012-4915
State	PUBLIC
Assigner	PSIRT-CNA@flexerasoftware.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2014-05-29 14:19:00 UTC
Updated	2017-08-29 01:32:00 UTC
Description	Directory traversal vulnerability in the Google Doc Embedder plugin before 2.5.4 for WordPress allows remote attackers to i

Risk And Classification

Problem Types: CWE-22

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Davistripe	Google Doc Embedder	2.0	All	All	All
Application	Davistripe	Google Doc Embedder	2.1	All	All	All
Application	Davistripe	Google Doc Embedder	2.2	All	All	All
Application	Davistripe	Google Doc Embedder	2.2.1	All	All	All
Application	Davistripe	Google Doc Embedder	2.2.2	All	All	All
Application	Davistripe	Google Doc Embedder	2.2.3	All	All	All
Application	Davistripe	Google Doc Embedder	2.3	All	All	All
Application	Davistripe	Google Doc Embedder	2.4	All	All	All
Application	Davistripe	Google Doc Embedder	2.4.1	All	All	All
Application	Davistripe	Google Doc Embedder	2.4.2	All	All	All
Application	Davistripe	Google Doc Embedder	2.4.3	All	All	All
Application	Davistripe	Google Doc Embedder	2.4.4	All	All	All
Application	Davistripe	Google Doc Embedder	2.4.5	All	All	All
Application	Davistripe	Google Doc Embedder	2.4.6	All	All	All
Application	Davistripe	Google Doc Embedder	2.5	All	All	All
Application	Davistripe	Google Doc Embedder	2.5.1	All	All	All
Application	Davistripe	Google Doc Embedder	2.5.2	All	All	All

Application	Davistripe	Google Doc Embedder	2.0	All	All	All
Application	Davistripe	Google Doc Embedder	2.1	All	All	All
Application	Davistripe	Google Doc Embedder	2.2	All	All	All
Application	Davistripe	Google Doc Embedder	2.2.1	All	All	All
Application	Davistripe	Google Doc Embedder	2.2.2	All	All	All
Application	Davistripe	Google Doc Embedder	2.2.3	All	All	All
Application	Davistripe	Google Doc Embedder	2.3	All	All	All
Application	Davistripe	Google Doc Embedder	2.4	All	All	All
Application	Davistripe	Google Doc Embedder	2.4.1	All	All	All
Application	Davistripe	Google Doc Embedder	2.4.2	All	All	All
Application	Davistripe	Google Doc Embedder	2.4.3	All	All	All
Application	Davistripe	Google Doc Embedder	2.4.4	All	All	All
Application	Davistripe	Google Doc Embedder	2.4.5	All	All	All
Application	Davistripe	Google Doc Embedder	2.4.6	All	All	All
Application	Davistripe	Google Doc Embedder	2.5	All	All	All
Application	Davistripe	Google Doc Embedder	2.5.1	All	All	All
Application	Davistripe	Google Doc Embedder	2.5.2	All	All	All
Application	Davistripe	Google Doc Embedder	All	All	All	All
Application	Wordpress	Wordpress	-	All	All	All
Application	Wordpress	Wordpress	-	All	All	All

References		
Reference	Source	Link
88891	OSVDB	osvdb.org
WordPress Google Doc Embedder Plugin Arbitrary File Disclosure Vulnerability	BID	www.bids.cve.org
IBM X-Force Exchange	XF	exchange.xforce.ibmcloud.com
Security Advisory SA50832 - WordPress Google Doc Embedder Plugin Arbitrary File Disclosure Vulnerability - Secunia	SECUNIA	secunia.com
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.

Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, completeness or usefulness of any information, opinion, advice or other content. EACH USER WILL BE SOLELY RESPONSIBLE FOR ANY consequences of his or her direct or indirect use of this web site. ALL WARRANTIES OF ANY KIND ARE EXPRESSLY DISCLAIMED. This site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE, CWE, and OVAL are registered trademarks of [The MITRE Corporation](#) and the authoritative source of CVE content is [MITRE's CVE web site](#). This site includes MITRE data granted under the following [license](#).

Free CVE JSON API cve.report/api

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