



CVE-2014-4549

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

Summary

CVE	CVE-2014-4549
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2014-07-02 20:55:00 UTC
Updated	2015-08-28 16:26:00 UTC
Description	Multiple cross-site scripting (XSS) vulnerabilities in pages/3DComplete.php in the WooCommerce SagePay Direct Payment Gateway Project

Risk And Classification

Problem Types: CWE-79

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Updated
Application	WooCommerce Sagepay Direct Payment Gateway Project	WooCommerce Sagepay Direct Payment Gateway	All	-

References

Reference	Source	Link
wp-plugins/sagepay-direct-for-woocommerce-payment-gateway · GitHub	CONFIRM	github.com
WordPress › WooCommerce SagePay Direct Payment Gateway « WordPress Plugins	CONFIRM	wordpress.org
wp-plugin : sagepay-direct-for-woocommerce-payment-gateway - A3-Cross-Site Scripting (XSS) - Code Vigilant	MISC	codevigilant.com
WordPress WooCommerce SagePay Direct Payment Gateway Plugin Cross Site Scripting Vulnerability	BID	www.securityfocus.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