



CVE-2012-5805

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

Summary

CVE	CVE-2012-5805
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2012-11-04 22:55:00 UTC
Updated	2012-11-06 05:00:00 UTC
Description	The PayPal IPN functionality in Zen Cart does not verify that the server hostname matches a domain name in the subject's

Risk And Classification

Problem Types: CWE-20

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Paypal	Instant Payment Notification	-	All	All	All
Application	Paypal	Instant Payment Notification	-	All	All	All
Application	Zen-cart	Zen Cart	-	All	All	All
Application	Zen-cart	Zen Cart	-	All	All	All

References

Reference	Source	Link	Tags
www.cs.utexas.edu/~shmat/shmat_ccs12.pdf	MISC	www.cs.utexas.edu	Exploit
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical, analysis

No vendor comments have been submitted for this CVE.

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

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](#).

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