CVE-2009-2254

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

Summary

CVE	CVE-2009-2254
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2009-06-30 10:30:00 UTC
Updated	2017-09-19 01:29:00 UTC
Description	Zen Cart 1.3.8a, 1.3.8, and earlier does not require administrative authentication for admin/sqlpatch.php, which allows remo

Risk And Classification

Problem Types: CWE-89

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Zen-cart	Zen Cart	1.1.0	All	All	All
Application	Zen-cart	Zen Cart	1.1.3	All	All	All
Application	Zen-cart	Zen Cart	1.2.0d	All	All	All
Application	Zen-cart	Zen Cart	1.2.1d	All	All	All
Application	Zen-cart	Zen Cart	1.2.4d	All	All	All
Application	Zen-cart	Zen Cart	1.3.6	All	All	All
Application	Zen-cart	Zen Cart	1.3.7	All	All	All
Application	Zen-cart	Zen Cart	1.3.8	All	All	All
Application	Zen-cart	Zen Cart	1.1.0	All	All	All
Application	Zen-cart	Zen Cart	1.1.3	All	All	All
Application	Zen-cart	Zen Cart	1.2.0d	All	All	All
Application	Zen-cart	Zen Cart	1.2.1d	All	All	All
Application	Zen-cart	Zen Cart	1.2.4d	All	All	All
Application	Zen-cart	Zen Cart	1.3.6	All	All	All
Application	Zen-cart	Zen Cart	1.3.7	All	All	All
Application	Zen-cart	Zen Cart	1.3.8	All	All	All
Application	Zen-cart	Zen Cart	All	All	All	All

References

Reference	Source	Link
Zen Cart Administration Security Bypass Vulnerability - Advisories - Community	SECUNIA	secunia.com
www.zen-cart.com/forum/attachment.php	CONFIRM	www.zen-cart.com
IBM X-Force Exchange	XF	exchange.xforce.ibmclo
55343	OSVDB	www.osvdb.org
Zen Cart 'admin/sqlpatch.php' SQL Injection Vulnerability	BID	www.securityfocus.com
IMPORTANT ADMIN SECURITY PATCH -- security_patch_v138_20090619.zip - Zen Cart Support	CONFIRM	www.zen-cart.com
Zen Cart 1.3.8 Remote SQL Execution Exploit	EXPLOIT-DB	www.exploit-db.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.