CVE-2009-2255

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

Summary

CVE	CVE-2009-2255
State	PUBLISHED
Assigner	mitre
Source Priority	CVE Program / NVD first with legacy fallback
Published	2009-06-30 10:30:19 UTC
Updated	2026-04-23 00:35:47 UTC
Description	Zen Cart 1.3.8a, 1.3.8, and earlier does not require administrative authentication for admin/record_company.php, which allo

Risk And Classification

Primary CVSS: v2.0 6.8 from nvd@nist.gov

AV:N/AC:M/Au:N/C:P/I:P/A:P

Problem Types: CWE-287 | n/a

CVSS v2.0 Breakdown

Access Vector

Network

Access Complexity

Medium

Authentication

None

Confidentiality

Partial

Integrity

Partial

Availability

Partial

AV:N/AC:M/Au:N/C:P/I:P/A:P

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	All	All	All	All

Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	Na	N/a	affected n/a	Not specified

References

Reference	Source
Zen Cart 1.3.8 Remote Code Execution Exploit	af854a3a-2127-422b-91ae-364da26611
www.zen-cart.com/forum/attachment.php	af854a3a-2127-422b-91ae-364da26611
IBM X-Force Exchange	af854a3a-2127-422b-91ae-364da26611
IMPORTANT ADMIN SECURITY PATCH -- security_patch_v138_20090619.zip - Zen Cart Support	af854a3a-2127-422b-91ae-364da26611
Zen Cart Administration Security Bypass Vulnerability - Advisories - Community	af854a3a-2127-422b-91ae-364da26611
www.osvdb.org/55344	af854a3a-2127-422b-91ae-364da26611
Zen Cart 'record_company.php' Remote Code Execution Vulnerability	af854a3a-2127-422b-91ae-364da26611
CVE Program record	CVE.ORG
NVD vulnerability detail	NVD

No vendor comments have been submitted for this CVE.

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