CVE-2014-6230

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

Summary

CVE	CVE-2014-6230
State	PUBLISHED
Assigner	mitre
Source Priority	CVE Program / NVD first with legacy fallback
Published	2014-10-25 00:55:03 UTC
Updated	2026-05-06 22:30:45 UTC
Description	WP-Ban plugin before 1.6.4 for WordPress, when running in certain configurations, allows remote attackers to bypass the II

Risk And Classification

Primary CVSS: v2.0 4.3 from nvd@nist.gov

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

Problem Types: CWE-20 | n/a

CVSS v2.0 Breakdown

Access Vector

Network

Access Complexity

Medium

Authentication

None

Confidentiality

Partial

Integrity

None

Availability

None

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

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Wp-ban Project	Wp-ban	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
WordPress › WP-Ban « WordPress Plugins	af854a3a-2127-
Vulnerability in WP-Ban allows visitors to bypass the IP blacklist in some configurations | dxwsecurity	af854a3a-2127-
Full Disclosure: Vulnerability in WP-Ban allows visitors to bypass the IP blacklist in some configurations (WordPress plugin)	af854a3a-2127-
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.