



CVE-2014-9034

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

Summary

CVE	CVE-2014-9034
State	PUBLISHED
Assigner	mitre
Source Priority	CVE Program / NVD first with legacy fallback
Published	2014-11-25 23:59:05 UTC
Updated	2026-05-06 22:30:45 UTC
Description	wp-includes/class-phpass.php in WordPress before 3.7.5, 3.8.x before 3.8.5, 3.9.x before 3.9.3, and 4.x before 4.0.1 allows

Risk And Classification

Primary CVSS: v2.0 5 from nvd@nist.gov

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

Problem Types: CWE-19 | n/a

CVSS v2.0 Breakdown

Access Vector

Network

Access Complexity

Low

Authentication

None

Confidentiality

None

Integrity

None

Availability

Partial

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

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Wordpress	Wordpress	3.8	All	All	All

Application	Wordpress	Wordpress	3.8.1	All	All	All
Application	Wordpress	Wordpress	3.8.2	All	All	All
Application	Wordpress	Wordpress	3.8.3	All	All	All
Application	Wordpress	Wordpress	3.8.4	All	All	All
Application	Wordpress	Wordpress	3.9	All	All	All
Application	Wordpress	Wordpress	3.9.1	All	All	All
Application	Wordpress	Wordpress	3.9.2	All	All	All
Application	Wordpress	Wordpress	4.0	All	All	All
Application	Wordpress	Wordpress	All	All	All	All

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

References
Reference
Debian -- Security Information -- DSA-3085-1 wordpress
403 Forbidden
WordPress › WordPress 4.0.1 Security Release
oss-security - Re: WordPress 4.0.1 Security Release
Support / Security / Advisories / / MDVSA-2014:233 Mandriva
Mageia Advisory: MGASA-2014-0493 - Updated wordpress package fixes security vulnerabilities
WordPress Bugs Let Remote Users Conduct Cross-Site Scripting, Cross-Site Request Forgery, and Denial of Service Attacks - SecurityTrack
CVE Program record
NVD vulnerability detail

No vendor comments have been submitted for this CVE.
There are currently no legacy QID mappings associated with this CVE.

