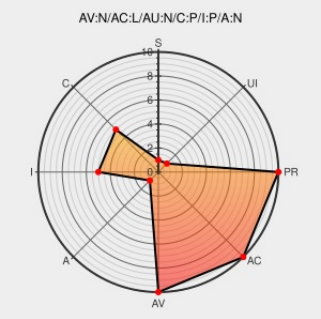
CVE-2014-9038

Published on: 11/25/2014 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:25:59 PM UTC

CVE-2014-9038

Source: Mitre | Source: NIST | CVE.ORG | Print: PDF



Certain versions of Wordpress from Wordpress contain the following vulnerability:

wp-includes/http.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 remote attackers to conduct server-side request forgery (SSRF) attacks by referring to a 127.0.0.0/8 resource.

CVE-2014-9038 has been assigned by cve@mitre.org to track the vulnerability

CVSS2 Score: 6.4 - MEDIUM

Access Vector	Access Complexity	Authentication
NETWORK	LOW	NONE
Confidentiality Impact	**Integrity Impact**	**Availability Impact**
PARTIAL	PARTIAL	NONE

CVE References

Description	Tags	Link
WordPress › WordPress 4.0.1 Security Release	Patch, Vendor Advisory, wordpress.org, text/html	CONFIRM wordpress.org/news/2014/11/wordpress-4-0-1/
oss-security - Re: WordPress 4.0.1 Security Release	openwall.com, text/html	MLIST [oss-security] 20141125 Re: WordPress 4.0.1 Security Release
Debian -- Security Information -- DSA-3085-1 wordpress	www.debian.org, Depreciated Link, text/html	DEBIAN DSA-3085
Support / Security / Advisories / / MDVSA-2014:233 | Mandriva	www.mandriva.com, text/html	MANDRIVA MDVSA-2014:233
Mageia Advisory: MGASA-2014-0493 - Updated wordpress package fixes security vulnerabilities	advisories.mageia.org, text/html	CONFIRM advisories.mageia.org/MGASA-2014-

		0493.html
WordPress Bugs Let Remote Users Conduct Cross-Site Scripting, Cross-Site Request Forgery, and Denial of Service Attacks - SecurityTracker	www.securitytracker.com text/html	SECTRACK 1031243
Changeset 30444 – WordPress Trac	Vendor Advisory web.archive.org text/html Inactive Link Not Archived	CONFIRM core.trac.wordpress.org/changeset/30444

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

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	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

cpe:2.3:a:wordpress:wordpress:3.8:*:*:*:*:*:*:*:

cpe:2.3:a:wordpress:wordpress:3.8.1:*:*:*:*:*:*:*:

cpe:2.3:a:wordpress:wordpress:3.8.2:*:*:*:*:*:*:*:

cpe:2.3:a:wordpress:wordpress:3.8.3:*:*:*:*:*:*:*:

cpe:2.3:a:wordpress:wordpress:3.8.4:*:*:*:*:*:*:*:

cpe:2.3:a:wordpress:wordpress:3.9:*:*:*:*:*:*:*:

cpe:2.3:a:wordpress:wordpress:3.9.1:*:*:*:*:*:*:*:

cpe:2.3:a:wordpress:wordpress:3.9.2:*:*:*:*:*:*:*:

cpe:2.3:a:wordpress:wordpress:4.0:*:*:*:*:*:*:*:

cpe:2.3:a:wordpress:wordpress:3.8:*:*:*:*:*:*:*:

cpe:2.3:a:wordpress:wordpress:3.8.1:*:*:*:*:*:*:*:

cpe:2.3:a:wordpress:wordpress:3.8.2:*:*:*:*:*:*:*:

cpe:2.3:a:wordpress:wordpress:3.8.3:*:*:*:*:*:*:*:

cpe:2.3:a:wordpress:wordpress:3.8.4:*:*:*:*:*:*:*:

cpe:2.3:a:wordpress:wordpress:3.9:*:*:*:*:*:*:*:

cpe:2.3:a:wordpress:wordpress:3.9.1:*:*:*:*:*:*:*:

cpe:2.3:a:wordpress:wordpress:3.9.2:*:*:*:*:*:*:*:

cpe:2.3:a:wordpress:wordpress:4.0:*:*:*:*:*:*:*:

cpe:2.3:a:wordpress:wordpress:*:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→