

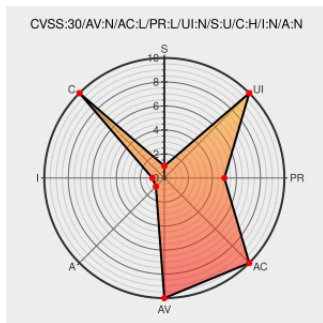


CVE-2017-14990

Published on: 10/02/2017 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:26:46 PM UTC

CVE-2017-14990

[Source: Mitre](#)[Source: NIST](#)[CVE.ORG](#)[Print: PDF](#) 

Certain versions of [Debian Linux](#) from [Debian](#) contain the following vulnerability:

WordPress 4.8.2 stores cleartext wp_signups.activation_key values (but stores the analogous wp_users.user_activation_key values as hashes), which might make it easier for remote attackers to hijack unactivated user accounts by leveraging database read access (such as access gained through an unspecified SQL injection vulnerability).

CVE-2017-14990 has been assigned by [M](#) cve@mitre.org to track the vulnerability - currently rated as **MEDIUM** severity.

CVSS3 Score: **6.5 - MEDIUM**

Attack Vector	Attack Complexity	Privileges Required	User Interaction
NETWORK	LOW	LOW	NONE
Scope	Confidentiality Impact	Integrity Impact	Availability Impact
UNCHANGED	HIGH	NONE	NONE

CVSS2 Score: **4 - MEDIUM**

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

CVE References

Description	Tags	Link
Debian -- Security Information -- DSA-3997-1 wordpress	Third Party Advisory www.debian.org Depreciated Link	DEBIAN DSA-3997

text/html

#38474 (wp_signups.activation_key stores activation keys in plain text) – WordPress Trac

Exploit

Issue Tracking

Third Party Advisory

web.archive.org

text/html

Inactive Link

Not Archived

MISC

core.trac.wordpress.org/ticket/38474

WordPress 'wp_signups.activation_key' Storage Method May Facilitate Remote Users in Hijacking User Accounts That Are Awaiting Activation - SecurityTracker

Third Party Advisory

VDB Entry

www.securitytracker.com

text/html

SECTrack 1039554

By selecting these links, you may be leaving CVEreport webspace. We have provided these links to other websites because they may have information that would be of interest to you. No inferences should be drawn on account of other sites being referenced, or not, from this page. There may be other websites that are more appropriate for your purpose. CVEreport does not necessarily endorse the views expressed, or concur with the facts presented on these sites. Further, CVEreport does not endorse any commercial products that may be mentioned on these sites. Please address comments about any linked pages to comment@cve.report.

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Debian	Debian Linux	8.0	All	All	All
Operating System	Debian	Debian Linux	9.0	All	All	All
Operating System	Debian	Debian Linux	8.0	All	All	All
Operating System	Debian	Debian Linux	9.0	All	All	All
Application	Wordpress	Wordpress	4.8.2	All	All	All
Application	Wordpress	Wordpress	4.8.2	All	All	All
cpe:2.3:o:debian:debian_linux:8.0:****:*:*:						
cpe:2.3:o:debian:debian_linux:9.0:****:*:*:						
cpe:2.3:o:debian:debian_linux:8.0:****:*:*:						
cpe:2.3:o:debian:debian_linux:9.0:****:*:*:						
cpe:2.3:a:wordpress:wordpress:4.8.2:****:*:*:						
cpe:2.3:a:wordpress:wordpress:4.8.2:****:*:*:						

No vendor comments have been submitted for this CVE

← Previous ID

Next ID →

© [CVE.report](#) 2023   |

Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, completeness or usefulness of any information, opinion, advice or other content. EACH USER WILL BE SOLELY RESPONSIBLE FOR ANY consequences of his or her direct or indirect use of this web site. ALL WARRANTIES OF ANY KIND ARE EXPRESSLY DISCLAIMED. This site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE, CWE, and OVAL are registered trademarks of [The MITRE Corporation](#) and the authoritative source of CVE content is [MITRE's CVE web site](#). This site includes MITRE data granted under the following [license](#).

CVE.report and Source URL Uptime Status [status.cve.report](#)