

roundcube / roundcubemail Public

- <> Code
- Issues 376
- Pull requests 69
- Discussions
- Actions
- Wiki




Commit 6d586cf

 **alecpl** committed 3 weeks ago

Fix pre-auth arbitrary file write via unsafe deserialization in redis/memcache session handler

Disable GuzzleHttp\Cookie\FileCookieJar instantiation.

Reported by y0us.

 **master** ·  1.7-rc6 1.7-rc5
 1 parent [122a2cd](#) commit 6d586cf 


 **2 files changed** +10 -0 lines changed

[↑ Top](#) 

Filter files...

 CHANGELOG.md

program/include

 inset.php

 **2 files changed** +10 -0 lines changed

Search within code

CHANGELOG.md



@@ -9,6 +9,7 @@ This file includes only changes we consider noteworthy for users, admins and plu

9 9 - Fix PHP fatal error when using IMAP cache (#10102)

10 10 - Fix Postgres connection using IPv6 address (#10104)

11 11 - Fix bug where `rel=stylesheet` part of a `` could get removed

12 + - Security: Fix pre-auth arbitrary file write via unsafe deserialization in redis/memcache session handler

12 13

13 14 ## 1.7-rc4

14 15



program/include/iniset.php



...

@@ -1,5 +1,7 @@

1 1 <?php

2 2

3 + use GuzzleHttp\Cookie\FileCookieJar;

4 +

3 5 /*

4 6 +-----+

5 7 | This file is part of the Roundcube Webmail client |



@@ -81,6 +83,13 @@

81 83 // register autoloader for rcmail app classes

82 84 spl_autoload_register('rcmail_autoload');

83 85

86 + // disable use of dangerous dependencies

87 + spl_autoload_register(static function (\$classname) {

88 + if (\$classname === FileCookieJar::class) {

89 + throw new \Exception("{classname} is forbidden for security reasons.");

90 + }

91 + }, true, true);

92 +

84 93 /**

85 94 * PHP5 autoloader routine for dynamic class loading

86 95 */



Comments 0



Please [sign in](#) to comment.