Commit 618c542

alecpl committed 2 weeks ago

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

Disable GuzzleHttp\Cookie\FileCookieJar instantiation.

Reported by y0us.
```

release-1.5 · 1.5.15 1.5.14

1 parent c15f5db commit 618c542

2 files changed +14 -1 lines changed

Top

Filter files...

- CHANGELOG.md
- program/include
  - iniset.php

2 files changed +14 -1 lines changed

Search within code

CHANGELOG.md

```
@@ -2,6 +2,10 @@

## Unreleased

+ - Security: Fix pre-auth arbitrary file write via unsafe deserialization in
  redis/memcache session handler
+
+ ## Release 1.5.13
+
```

```
5   9   - Fix remote image blocking bypass via SVG content reported by nullcathedral
6   10  - Fix CSS injection vulnerability reported by CERT Polska
7   11
```

program/include/iniset.php

```
    ...   @@ -1,6 +1,8 @@
1   1     <?php
2   2
3       - /**
        3 + use GuzzleHttp\Cookie\FileCookieJar;
        4 +
        5 + /*
4   6      +--------------------------------------------------------------------+
5   7      | This file is part of the Roundcube Webmail client                  |
6   8      |                                                                    |
    ...   @@ -76,6 +78,13 @@
76  78    // register autoloader for rcmail app classes
77  79    spl_autoload_register('rcmail_autoload');
78  80
        81 + // disable use of dangerous dependencies
        82 + spl_autoload_register(static function ($classname) {
        83 +     if ($classname === FileCookieJar::class) {
        84 +         throw new \Exception("{$classname} is forbidden for security reasons.");
        85 +     }
        86 + }, true, true);
        87 +
79  88    /**
80  89     * PHP5 autoloader routine for dynamic class loading
81  90     */
```

Comments 0

Please sign in to comment.