[KIS-2022-01] ImpressCMS <= 1.4.2 (autologin.php) Authentication Bypass Vulnerability

From: Egidio Romano <research () karmainsecurity com>
Date: Tue, 22 Mar 2022 13:00:53 +0100

```
-----------------------------------------------------------------------
ImpressCMS <= 1.4.2 (autologin.php) Authentication Bypass Vulnerability
-----------------------------------------------------------------------
```

[-] Software Link:

https://www.impresscms.org

[-] Affected Versions:

Version 1.4.2 and prior versions.

[-] Vulnerability Description:

The vulnerability is located in the /plugins/preloads/autologin.php script:

```
45.            $uname = $myts->stripSlashesGPC($autologinName);
46.            $pass = $myts->stripSlashesGPC($autologinPass);
47.            if (empty($uname) || is_numeric($pass)) {
48.                $user = false ;
49.            } else {
50.                // V3
51.                $uname4sql = addslashes($uname);
52.                $criteria = new icms_db_criteria_Compo(new icms_db_criteria_Item('login_name', $uname4sql));
53.                $user_handler = icms::handler('icms_member_user');
54.                $users = $user_handler->getObjects($criteria, false);
55.                if (empty($users) || count($users) != 1) {
56.                    $user = false ;
57.                } else {
58.                    // V3.1 begin
59.                    $user = $users[0] ;
60.                    $old_limit = time() - (defined('ICMS_AUTOLOGIN_LIFETIME') ? ICMS_AUTOLOGIN_LIFETIME : 604800);
61.                    list($old_Ynj, $old_encpass) = explode(':', $pass);
62.                    if (strtotime($old_Ynj) < $old_limit || md5($user->getVar('pass') . 63.
    ICMS_DB_PASS . ICMS_DB_PREFIX . $old_Ynj) != $old_encpass)
64.                    {
65.                        $user = false;
66.                    }
```

User input passed through the "autologin_uname" and "autologin_pass" cookie values is being used at lines 51-54 to fetch an user object from the database, and then at lines 62-63 to check the correctness of the user's password. The vulnerability exists because of an unsafe way of comparing those parameters, due to comparison operator != is being used instead of !== within the "if" statement at lines 62-63. The latter operator returns "true" only if the compared values are equal and the same type, while the first compares the values after "type juggling". This might be exploited to potentially bypass the authentication mechanism and login as any user without the knowledge of the password.

[-] Solution:

Upgrade to version 1.4.3 or later.

[-] Disclosure Timeline:

[20/01/2021] - Vendor notified through HackerOne
[02/02/2021] - Vendor replied this has been resolved and will be in ImpressCMS 1.4.3
[03/02/2021] - CVE number assigned
[06/02/2022] - Version 1.4.3 released
[22/03/2022] - Public disclosure

[-] CVE Reference:

The Common Vulnerabilities and Exposures project (cve.mitre.org)
has assigned the name CVE-2021-26600 to this vulnerability.

[-] Credits:

Vulnerability discovered by Egidio Romano.

[-] Other References:

https://hackerone.com/reports/1081986

[-] Original Advisory:

http://karmainsecurity.com/KIS-2022-01

____
Sent through the Full Disclosure mailing list
https://nmap.org/mailman/listinfo/fulldisclosure
Web Archives & RSS: http://seclists.org/fulldisclosure/