ImpressCMS 1.4.2 Authentication Bypass

Authored by EgiX | Site karmainsecurity.com

Posted Mar 22, 2022

ImpressCMS versions 1.4.2 and below suffer from an authentication bypass vulnerability.

tags | exploit, bypass
advisories | CVE-2021-26600
SHA-256 | d8dfe7df740ddc2041569cf9735ee4180779ccae9c55e66d12ed7119dce09379

Download | Favorite | View

Related Files

Share This

Like Twee LinkedIn Reddit Digg StumbleUpon

Change Mirror Download

```
------------------------------------------------------------------------
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
```

Login or Register to add favorites

Follow us on Twitter

Subscribe to an RSS Feed

File Archive: December 2022 <

Su	Mo	Tu	We	Th	Fr	Sa
				1	2	3
4	5	6	7	8	9	10
11	12	13	14	15	16	17
18	19	20	21	22	23	24
25	26	27	28	29	30	31

Top Authors In Last 30 Days

Red Hat 201 files
Ubuntu 78 files
Debian 24 files
LiquidWorm 23 files
malvuln 12 files
nu11secur1ty 11 files
Gentoo 9 files
Google Security Research 8 files
T. Weber 4 files
Julien Ahrens 4 files

File Tags

ActiveX (932)
Advisory (79,754)
Arbitrary (15,694)
BBS (2,859)
Bypass (1,619)
CGI (1,018)
Code Execution (6,926)
Conference (673)
Cracker (840)
CSRF (3,290)
DoS (22,602)
Encryption (2,349)
Exploit (50,359)
File Inclusion (4,165)
File Upload (946)
Firewall (821)
Info Disclosure (2,660)
Intrusion Detection (867)
Java (2,899)
JavaScript (821)
Kernel (6,291)
Local (14,201)
Magazine (586)
Overflow (12,419)
Perl (1,418)
PHP (5,093)
Proof of Concept (2,291)
Protocol (3,435)
Python (1,467)
Remote (30,044)
Root (3,504)
Ruby (594)
Scanner (1,631)
Security Tool (7,777)
Shell (3,103)
Shellcode (1,204)
Sniffer (886)

File Archives

December 2022
November 2022
October 2022
September 2022
August 2022
July 2022
June 2022
May 2022
April 2022
March 2022
February 2022
January 2022
Older

Systems

AIX (426)
Apple (1,926)
BSD (370)
CentOS (55)
Cisco (1,917)
Debian (6,634)
Fedora (1,690)
FreeBSD (1,242)
Gentoo (4,272)
HPUX (878)
iOS (330)
iPhone (108)
IRIX (220)
Juniper (67)
Linux (44,315)
Mac OS X (684)
Mandriva (3,105)
NetBSD (255)
OpenBSD (479)
RedHat (12,469)
Slackware (941)
Solaris (1,607)

Spoof (2,166)
SQL Injection (16,102)
TCP (2,379)
Trojan (686)
UDP (876)
Virus (662)
Vulnerability (31,136)
Web (9,365)
Whitepaper (3,729)
x86 (946)
XSS (17,494)
Other

SUSE (1,444)
Ubuntu (8,199)
UNIX (9,159)
UnixWare (185)
Windows (6,511)
Other

Site Links
News by Month
News Tags
Files by Month
File Tags
File Directory

About Us
History & Purpose
Contact Information
Terms of Service
Privacy Statement
Copyright Information

Hosting By
Rokasec

Follow us on Twitter

Subscribe to an RSS Feed