ImpressCMS 1.4.2 Incorrect Access Control

Authored by EgiX | Site karmainsecurity.com

Posted Mar 22, 2022

ImpressCMS versions 1.4.2 and below suffer from an incorrect access control vulnerability.

tags | exploit
advisories | CVE-2021-26598
SHA-256 | 4b55169e7ddd7a9da312a1bb940bbd4357b7a28a5e228523903848b5c2e04d5f Download | Favorite | View

Related Files

Share This

Like Twee LinkedIn Reddit Digg StumbleUpon

Change Mirror Download

```
------------------------------------------------------------------------
ImpressCMS <= 1.4.2 (findusers.php) Incorrect Access Control Vulnerability
------------------------------------------------------------------------


[-] Software Link:

https://www.impresscms.org


[-] Affected Versions:

Version 1.4.2 and prior versions.


[-] Vulnerability Description:

The vulnerability is located in the /include/findusers.php script:

16.    include "../mainfile.php";
17.    xoops_header(false);
18.
19.    $denied = true;
20.    if (!empty($_REQUEST['token'])) {
21.        if (icms::$security->validateToken($_REQUEST['token'], false)) {
22.            $denied = false;
23.        }
24.    } elseif (is_object(icms::$user) && icms::$user->isAdmin()) {
25.        $denied = false;
26.    }
27.    if ($denied) {
28.        icms_core_Message::error(_NOPERM);
29.        exit();
30.    }        }

This script should be accessible to authenticated users only. However,
because of the "if" statement at lines 20-23, this script could be
accessed by unauthenticated attackers if they will provide a valid
security token. Such a token will be generated in several places within
the application, and some of them do not require the user to be
authenticated, like in the misc.php script. This might be exploited to
access an otherwise restricted functionality of the application, which
in turn might allow an information disclosure about the CMS users.


[-] Solution:

Upgrade to version 1.4.3 or later.


[-] Disclosure Timeline:

[19/01/2021] - Vendor notified through HackerOne
[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-2021-26598 to this vulnerability.


[-] Credits:

Vulnerability discovered by Egidio Romano.


[-] Other References:

https://hackerone.com/reports/1081137


[-] Original Advisory:

http://karmainsecurity.com/KIS-2022-03
```


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