# ImpressCMS 1.4.2 Path Traversal

Authored by EgiX | Site karmainsecurity.com

Posted Mar 22, 2022

ImpressCMS versions 1.4.2 and below suffer from a path traversal vulnerability that can allow for arbitrary file deletion.

tags | exploit, arbitrary
advisories | CVE-2021-26601
SHA-256 | 54cb7c2588875cdae13b83017043e25037564efb357fe49a475251f02139a0d4

Download | Favorite | View

Related Files

Share This

Like Twee LinkedIn Reddit Digg StumbleUpon

Change Mirror Download

```
-------------------------------------------------------------------
ImpressCMS <= 1.4.2 (image-edit.php) Path Traversal Vulnerability
-------------------------------------------------------------------


[-] Software Link:

https://www.impresscms.org


[-] Affected Versions:

Version 1.4.2 and prior versions.


[-] Vulnerability Description:

The vulnerability is located in the
/libraries/image-editor/image-edit.php script:

161.        if (@copy ( ICMS_IMANAGER_FOLDER_PATH . '/temp/' .
$simage_temp, $categ_path . $simage->getVar ( 'image_name' ) )) {
162.            if (@unlink ( ICMS_IMANAGER_FOLDER_PATH . '/temp/' .
$simage_temp )) {
163.                $msg = _MD_AM_DBUPDATED;

[...]

190.        } else {
191.            if (copy ( ICMS_IMANAGER_FOLDER_PATH . '/temp/' .
$simage_temp, $categ_path . $imgname )) {
192.                @unlink ( ICMS_IMANAGER_FOLDER_PATH . '/temp/' .
$simage_temp );
193.            }

User input passed through the "image_temp" parameter is not properly
sanitized before being used in a call to the unlink() function at lines
162 and 192. This can be exploited by authenticated attackers to carry
out Path Traversal attacks and delete arbitrary files in the context of
the web server process. This vulnerability could be exploited also to
disclose the content of arbitrary files in case the web server allows
for directory listing.

[-] Solution:

Upgrade to version 1.4.3 or later.


[-] Disclosure Timeline:

[19/01/2021] - Vendor notified through HackerOne
[29/01/2021] - Vulnerability acknowledged by the vendor
[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-2021-26601 to this vulnerability.


[-] Credits:

Vulnerability discovered by Egidio Romano.


[-] Other References:

https://hackerone.com/reports/1081878


[-] Original Advisory:

http://karmainsecurity.com/KIS-2022-02
```

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