Search .

Home Files News About Contact &[SERVICES_TAB]

Add New

flatCore CMS XSS / File Disclosure / SQL Injection

Authored by Calvin Phang, Yew Chung Cheah | Site sec-consult.com

Posted Jan 13, 2021

flatCore CMS versions prior to 2.0.0 build 139 suffer from cross site scripting, file disclosure, and remote SQL injection vulnerabilities.

tags | exploit remote vulnerability xss sql injection

ries | CVE-2021-23835, CVE-2021-23836, CVE-2021-23838

Related Files

Follow us on Twitter Subscribe to an RSS Feed

File Archive: December 2022 < Mo Tu We Th Sa 1 3 5 6 7 8 10 11 12 13 14 15 17 19 20 21 22 23 18 24 26 27 28 29 30 25 31

-	
Top /	Authors In Last 30 Days
Red H	at 201 files
Ubunt	u 78 files
Debiar	1 24 files
Liquid	Worm 23 files
malvul	In 12 files
nu11se	ecur1ty 11 files
Gento	0 9 files
Google	e Security Research 8 files
T. Web	er 4 files
Julien	Ahrens 4 files

File Archives File Tags December 2022 ActiveX (932) Advisory (79,754) Arbitrary (15.694) October 2022 RRS (2.859) September 2022 August 2022 Bypass (1,619) CGI (1,018) July 2022 Code Execution (6,926) June 2022 Conference (673) May 2022 April 2022 Cracker (840) March 2022 CSRF (3,290) DoS (22 602) February 2022 Encryption (2,349) January 2022 Exploit (50,359) Older File Inclusion (4,165) File Upload (946) Systems Firewall (821) AIX (426) Info Disclosure (2,660) Apple (1,926) Intrusion Detection (867) BSD (370) Java (2.899) CentOS (55) JavaScript (821) Cisco (1.917) Kernel (6,291) Debian (6,634) Local (14.201) Magazine (586) FreeBSD (1.242) Gentoo (4.272) Perl (1.418) HPUX (878) PHP (5.093) iOS (330) Proof of Concept (2,291) iPhone (108) Protocol (3,435) IRIX (220) Python (1.467) Juniper (67) Remote (30,044) Linux (44,315) Mac OS X (684) Ruby (594) Mandriva (3.105) Scanner (1.631) Security Tool (7,777) OpenBSD (479) Shell (3,103) RedHat (12,469) Shellcode (1,204) Slackware (941) Sniffer (886) Solaris (1,607)

Share This								
Lik€	TWEE	LinkedIn	Reddit	Digg	StumbleUpon			
Change Mirror						Download		
SEC Consult Vulnerability Lab Security Advisory < 20210113-1 > title: Multiple Vulnerabilities product: flatCore CMS vulnerable version: < 2.0.0 Build 139 flxed version: Release 2.0.0 Build 139 CVE. number: CVF. 2021-23836, CVF. 2021-23836, CVE. 2021-23837, CVE. 2021-23838 Domepage: https://flatCore.org/ found: 2020-01-20 build: Vew Chung Cheah (Office Singapore) Calvin Phang (Office Singapore) SEC Consult Vulnerability Lab								
An integrated part of SEC Consult, an Atos company Europe Asia North America								
	https://www.sec-co	onsult.com						
Vendor description:								
"flatCore is based of possible, but can be looking for a soluti may be your buddy."	easily extended by	the modular s	structure. If	you are				
Source: https://flat	core.org/							
Business recommendat	ion:							
The vendor provides								
An in-depth security advised, as the soft								
Vulnerability overview/description:								
1) Reflected Cross-S A reflected cross-si HTTP request body ps accepts malicious cl example, a malicious from a victim user a unauthorized access	te scripting vulner rameter for the 'ac ient side script wi user can leverage nd perform a session	ability was id p' interface. ithout proper i this vulnerabi	dentified in The affected input sanitiz ility to stea	the 'media_ parameter ation. For 1 cookies				
2) Stored Cross-Site Scripting (Authenticated user) (CVE-2021-23936) A stored cross-site scripting vulnerability was identified in the 'prefa_smtp_psw' HTTP request body parameter for the 'acp' interface. An admin user can inject malicious client side script to the affected parameter without any form of input sanitization. The injected payload will be executed in the browser of a user whenever one visits the affected module page.								
3) Local File Disclosure (Authenticated user) (CVE-2021-2385) A local file disclosure vulnerability was identified in the 'doca file' HTTP request body parameter for the 'acp' interface which can be exploited with admin access rights. The affected parameter which retrieves the contents of the specified file was found to be accepting malicious user inputs without proper input sanitization, thus leading to retrieval of backend server sensitive files, for example /etc/passwd, sqlite database files, FWF source code etc.								
4) Time Based Blind SQL Injection (Authenticated user) (CVE-2021-23837) A time based blind SQL injection was identified in the 'selected folder' HTTP request body parameter for the 'acp' interface. The affected parameter which retrieves the file contents of the specified folder was found to be accepting malicious user inputs without proper input sanitization, thus leading to SQL injection. Database related information can be successfully retrieved.								

1) Reflected Cross-Site Scripting (Authenticated user) (CVE-2021-23838) An authenticated admin user can exploit this vulnerability by manipulating the 'media filter' parameter found in the Files' Manage Files module.

Stored Cross-Site Scripting (Authenticated user) (CVE-2021-23836)
 An authenticated admin user can exploit this vulnerability by manipulating the 'prefs_sutp_psw' parameter found in the System' E-Mail module.

3) Local File Disclosure (Authenticated user) (CVE-2021-23835) An authenticated admin user can exploit this vulnerability by manipulating the 'docs_file' parameter found in the help module.

4) Time Based Blind SQL Injection (Authenticated user) (CVE-2021-23837) An authenticated admin user can exploit this vulnerability by manipulation the 'selected folder' parameter found in the Files' Manage Files module.

URL: http://\$HOST/acp/acp.php?tn-filebrowser&sub-browse
METHOD: POST
PARAMETER: selected_folder
PAYLOAD: 2* AND 8483-LIKE(*ABCDEFG',UPPER(HEX(RANDOMBLOB(500000000/2)))) AND 'eJQr%'='eJQr

flatCore CMS version 2.0.0 (Build 122) has been tested, which was the latest version available at the time of the test. Previous versions may also be affected.

PARAMETER: prefs_smtp_psw
PAYLOAD: '%3e%3cscript%3ealert(document.cookie)%3c%2fscript%3eaaabbb

2020-12-14 | Contacting vendor through support@flatcore.de 2020-12-17 | Advisory sent to the vendor 2020-12-31 | Requesting status update from vendor

URL: http://\$HOST/acp/acp.php?tn=filebrowser&sub=browse
METHOD: POST
PARAMETER: media_filter
PAYLOAD: asast@scriptt3ealert(document.cookie)%3c%2fscript%3ebbb

URL : http://\$HOST/acp/acp.php?tn=system&sub=mail METHOD : POST

URL : http://\$HOST/acp/acp.php METHOD : POST

TCP (2,379) UNIX (9,159)
Trojan (886) UnixWare (185)
UDP (876) Windows (6,511)
Virus (662) Other
Vulnerability (31,136)
Web (9,365)
Whitepaper (3,729)
x86 (946)
XSS (17,494)
Other

SQL Injection (16,102) Ubuntu (8,199)

SUSE (1,444)

Spoof (2,166)

Login or Register to add favorites



Site Links About Us

News by Month History & Purpose

News Tags Contact Information

Files by Month Terms of Service

File Tags Privacy Statement
File Directory Copyright Information

Hosting By

Rokasec



