Date: Fri, 7 Aug 2020 20:43:18 +0000
From: SEC Consult Vulnerability Lab <research@...-consult.com>
To: "fulldisclosure@...lists.org" <fulldisclosure@...lists.org>
Subject: [FD] SEC Consult SA-20200807-0 :: Multiple Vulnerabilities in flatCore CMS

SEC Consult Vulnerability Lab Security Advisory < 20200807-0 >
==
title: Multiple Vulnerabilities
product: flatCore CMS
vulnerable version: <=1.5.5
fixed version: 1.5.7
CVE number: -
impact: High
homepage: https://flatcore.org/
found: 2020-03-28
by: Farhan Rahman (Office Malaysia)
Azrul Ikhwan Zulkifli (Office Malaysia)
SEC Consult Vulnerability Lab

An integrated part of SEC Consult
Europe | Asia | North America

https://www.sec-consult.com

==

Vendor description:

"flatCore is based on PHP and PDO/SQLite. The Core is as
minimalistic as possible, but can be easily extended by
the modular structure. If you are looking for a solution
to edit your website live and with ease, flatCore may be
your buddy."

Source: https://flatcore.org/

Business recommendation:

Update to the latest version of flatCore CMS.
An in-depth security analysis performed by security professionals is highly
advised, as the software may be affected from further security issues.

Vulnerability overview/description:
----
1. Stored Cross Site Scripting (Authenticated user)
This vulnerability allows an authenticated user (admin) to inject a malicious
client side script which will be executed in the browser of a user if he
visits the manipulated URL.
In this case, the payload will be executed when the user visits any page that
contains the injected malicious client side script.

2. Upload of arbitrary files (Authenticated user)
It was identified that an authenticated user (admin) has the possibility to
upload malicious files without any restriction. In this specific case,
arbitrary server side PHP code such as web shells can be uploaded. As a result
the attacker can run arbitrary code on the server side with the privileges of
the web server. This could lead to a full system compromise.

Proof of concept:
----
1. Stored Cross Site Scripting (Authenticated user)
The following parameters have been found to be vulnerable to
stored cross site scripting attacks.

(a)
URL : http://$DOMAIN/acp/acp.php?tn=pages&sub=edit&editpage=1
METHOD : POST
PARAMETER : page_linkname, page_title, page_content, page_extracontent
PAYLOAD : aaaa%3Cscript%3Ealert%28document.cookie%29%3C%2Fscript%3E

Go to http://$DOMAIN/ , and the XSS will be executed.

(b)
URL : http://$DOMAIN/acp/acp.php?tn=system&sub=sys_pref
METHOD : POST
PARAMETER : prefs_pagename, prefs_pagetitle, prefs_pagesubtitle
PAYLOAD : aaaa%3Cscript%3Ealert%28document.cookie%29%3C%2Fscript%3E

Go to http://$DOMAIN/ , and the XSS will be executed.

2. Upload of arbitrary files (Authenticated user)
Go to Upload Files > Choose destination > files.

Upload a desired PHP web shell as the shell.php file.

Once uploaded, to execute the webshell, go to
http://$DOMAIN/content/files/shell.php

Vulnerable / tested versions:
----
flatCore CMS version 1.5.5 has been tested, which was the latest version
available at the time of the test. Previous versions may also be affected.

Vendor contact timeline:

2020-04-02: Contacting vendor through support@...tcore.org.
2020-04-28: Vendor developer asked for details. Sending details.
2020-06-02: Follow-up with vendor; no response.
2020-06-08: Follow-up with vendor; no response.
2020-06-10: Vendor requested to give them some times to patch
the vulnerabilities.
2020-07-10: Follow-up with vendor; no response.
2020-07-22: Vendor fixed the reported issues, and release the new version
(1.5.7) at their website.
2020-08-07: Public release of security advisory

Solution:

The fixed version 1.5.7 is available at the vendor's download section:
* https://flatcore.org/downloads/

Workaround:

None

Advisory URL:
----
https://sec-consult.com/en/vulnerability-lab/advisories/index.html

~~~~~~

SEC Consult Vulnerability Lab

SEC Consult
Europe | Asia | North America

About SEC Consult Vulnerability Lab
The SEC Consult Vulnerability Lab is an integrated part of SEC Consult. It
ensures the continued knowledge gain of SEC Consult in the field of network
and application security to stay ahead of the attacker. The SEC Consult
Vulnerability Lab supports high-quality penetration testing and the evaluation
of new offensive and defensive technologies for our customers. Hence our
customers obtain the most current information about vulnerabilities and valid
recommendation about the risk profile of new technologies.

~~~~~~
Interested to work with the experts of SEC Consult?
Send us your application https://sec-consult.com/en/career/index.html

Interested in improving your cyber security with the experts of SEC Consult?
Contact our local offices https://www.sec-consult.com/en/contact/index.html
~~~~~~

Mail: research at sec-consult dot com
Web: https://www.sec-consult.com
Blog: http://blog.sec-consult.com
Twitter: https://twitter.com/sec_consult

EOF F. Rahman, A. Zulkifli / @2020

_____
Sent through the Full Disclosure mailing list
https://nmap.org/mailman/listinfo/fulldisclosure
Web Archives & RSS: http://seclists.org/fulldisclosure/

Powered by blists - more mailing lists

OPENWALL OPENVZ
~~~~~~