

Search ...

CMS Made Simple 2.2.14 Cross Site Scripting

Authored by [Roel van Beurden](#)

Posted Oct 1, 2020

CMS Made Simple version 2.2.14 suffers from a persistent cross site scripting vulnerability.

tags | [exploit](#), [xss](#)

advisories | [CVE-2020-24860](#)

SHA-256 | 5752983fb6f8ef3b1665360cb1a3d3b1151ff77e75d6c1e7b6e22ee07860149c [Download](#) | [Favorite](#) | [View](#)

Related Files

Share This

Like

Twitter

LinkedIn

Reddit

Digg

StumbleUpon

Change MirrorDownload

Exploit Title: CMS Made Simple 2.2.14 - Persistent Cross-Site Scripting (Authenticated)
Google Dork: -
Date: 2020-09-29
Exploit Author: Roel van Beurden
Vendor Homepage: <https://www.cmsmadesimple.org/>
Software Link: <http://s3.amazonaws.com/cmsma/downloads/14793/cmsma-2.2.14-install.zip>
Version: 2.2.14
Tested on: Linux Ubuntu 18.04
CVE: CVE-2020-24860

1. Description:

CMS Made Simple 2.2.14 allows an authenticated user with access to the Content Manager to edit content and put persistent XSS payload in the affected text fields. The user can get cookies from every authenticated user who visits the website.

2. Affected parameters:

Content > Content Manager > Edit some page > Logic (tab) > Page Specific Metadata (text field)
Content > Content Manager > Edit some page > Logic (tab) > Smart data or logic that is specific to this page (text field)

3: Example payload:

<script>alert(document.cookie);</script>

4: Exploitation demo:

youtube.com/watch?v=M6D7DmmjLak&t=22s

[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

nu11security 11 files

Gentoo 9 files

Google Security Research 6 files

Julien Ahrens 4 files

T. Weber 4 files

File Tags

ActiveX (932)	December 2022
Advisory (79,754)	November 2022
Arbitrary (15,694)	October 2022
BBS (2,859)	September 2022
Bypass (1,619)	August 2022
CGI (1,018)	July 2022
Code Execution (8,926)	June 2022
Conference (673)	May 2022
Cracker (840)	April 2022
CSRF (3,290)	March 2022
DoS (22,602)	February 2022
Encryption (2,349)	January 2022
Exploit (50,359)	Older
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