

Composr CMS 10.0.30 Cross Site Scripting

Authored by Manuel Garcia Cardenas

Posted May 20, 2020

Composr CMS version 10.0.30 suffers from a persistent cross site scripting vulnerability.

tags | exploit, xss

advisories | CVE-2020-8789

SHA-256 | bd0304dc55718b3129060de9dd8a6ac6f198948bfb00573ed86879db126f081e Download | Favorite | View

Related Files

Share This

Like

Twitter

LinkedIn

Reddit

Digg

StumbleUpon

Change Mirror Download

Title: Composr CMS 10.0.30 - Persistent Cross-Site Scripting
Author: Manuel Garcia Cardenas
Date: 2020-02-06
Vendor: https://compo.sz/
CVE: N/A

MGC ALERT 2020-001
- Original release date: February 06, 2020
- Last revised: May 21, 2020
- Discovered by: Manuel Garcia Cardenas
- Severity: 4,8/10 (CVSS Base Score)
- CVE-ID: CVE-2020-8789

I. VULNERABILITY

Composr CMS 10.0.30 - (Authenticated) Cross-Site Scripting

II. BACKGROUND

Composr CMS (or Composr) is a web application for creating websites. It is a combination of a Web content management system and Online community (Social Networking) software. Composr is licensed as free software and primarily written in the PHP programming language.

III. DESCRIPTION

Has been detected a Persistent XSS vulnerability in Composr CMS, that allows the execution of arbitrary HTML/script code to be executed in the context of the victim user's browser.

IV. PROOF OF CONCEPT

Go to: Security -> Usergroups -> Edit Usergroup

Select one Usergroup (for example Guest) and edit the Name (parameter name) for example with Guests"><script>alert(1)</script>

The variable "name" it is not sanitized, later, if some user visit the "Zone editor" area, the XSS is executed, in the response you can view:

<input type="hidden" name="label_for_access_1" value="Access for Guests"><script>alert(1)</script>" />

V. BUSINESS IMPACT

An attacker can execute arbitrary HTML or Javascript code in a targeted user's browser, this can leverage to steal sensitive information as user credentials, personal data, etc.

VI. SYSTEMS AFFECTED

Composr CMS <= 10.0.30

VII. SOLUTION

Disable until a fix is available.

VIII. REFERENCES

https://compo.sz/

IX. CREDITS

This vulnerability has been discovered and reported by Manuel Garcia Cardenas (advidsec (at) gmail (dot) com).

X. REVISION HISTORY

February 06, 2020 1: Initial release
May 21, 2020 2: Last revision

XI. DISCLOSURE TIMELINE

February 06, 2020 1: Vulnerability acquired by Manuel Garcia Cardenas
February 06, 2020 2: Send to vendor
April 06, 2020 3: New request, vendor doesn't answer.
May 21, 2020 4: Sent to lists

XII. LEGAL NOTICES

The information contained within this advisory is supplied "as-is" with no warranties or guarantees of fitness of use or otherwise.

XIII. ABOUT

Manuel Garcia Cardenas
Pentester

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)

Advisory (79,754)

Arbitrary (15,694)

BBS (2,859)

Bypass (1,619)

CGI (1,018)

Code Execution (8,926)

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



© 2022 Packet Storm. All rights reserved.

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