Composr CMS 10.0.30 - (Authenticated) Cross-Site Scripting

From: Manuel Garcia Cardenas <advidsec () gmail com>
Date: Thu, 21 May 2020 10:15:35 +0200

```
================================================
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.sr/

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

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

By Date By Thread

Current thread:

Composr CMS 10.0.30 - (Authenticated) Cross-Site Scripting *Manuel Garcia Cardenas (May 22)*