Zenario CMS 8.8.52729 SQL Injection

Authored by Avinash R

Posted Jun 11, 2021

Zenario CMS version 8.8.52729 suffers from authenticated blind and error-based remote SQL injection vulnerabilities.

tags | exploit, remote, vulnerability, sql injection
advisories | CVE-2021-27673
SHA-256 | 11f07b628a0a72c6c3d47e19afb655ba368abd52566f0f3123bace80ce1559b9 Download | Favorite | View

Related Files

Share This

Like Twee LinkedIn Reddit Digg StumbleUpon

Change Mirror Download

```
# Exploit Title: Zenario CMS 8.8.52729 - 'cID' Blind & Error based SQL injection (Authenticated)
# Date: 05-02-2021
# Exploit Author: Avinash R
# Vendor Homepage: https://zenar.io/
# Software Link: https://github.com/TribalSystems/Zenario/releases/tag/8.8
# Version: 8.8.52729
# Tested on: Windows 10 Pro (No OS restrictions)
# CVE : CVE-2021-27673
# Reference: https://deadsh0t.medium.com/blind-error-based-authenticated-sql-injection-on-zenario-8-8-52729-
cms-d4705534df38

##### Step To Reproduce #####

1) Login to the admin page of Zenario CMS with admin credentials, which is
http://server_ip/zenario/admin.php

2) Click on, New → HTML page to create a new sample page and intercept it
with your interceptor.

3) Just a single quote on the 'cID' parameter will confirm the SQL
injection.

4) After confirming that the 'cID' parameter is vulnerable to SQL
injection, feeding the request to SQLMAP will do the rest of the work for
you.

############ End ############
```

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 157 files
Ubuntu 76 files
LiquidWorm 23 files
Debian 21 files
nu11secur1ty 11 files
malvuln 11 files
Gentoo 9 files
Google Security Research 8 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