

Search . Home Files News About Contact &[SERVICES_TAB] Add New

Zenario CMS 8.8.52729 SQL Injection

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 ies | CVE-2021-27673

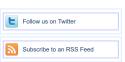
Related Files

Share This

LinkedIn Reddit Digg StumbleUpon Like TWO

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
Exploit Author: Avinash R
Vendor Rempage: https://zenar.io/
Software Link: https://glthub.com/FribalSystems/Zenario/releases/tag/8.8
Version: 8.052729
Version: 8.052729
Town CVD-201-27810 Pro (No OS restrictions)
Town CVD-201-27810 Pro (No OS restrictions)
Town CVD-201-27810 Pro (No OS restrictions)
Reference: https://deadsh0t.medium.com/blind-error-based-authenticated-sql-injection-on-zenario-8-8-52729cms-04705354d438 #### Step To Reproduce #### Login to the admin page of Zenario CMS with admin credentials, which is http://server_ip/zenario/admin.php 2) Click on, ${\tt New} \rightarrow {\tt HTML}$ 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. 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





Top Authors In Last 30 Days Red Hat 157 files Ubuntu 76 files LiquidWorm 23 files Debian 21 files nu11secur1ty 11 files Gentoo 9 files Google Security Research 8 files Julien Ahrens 4 files T. Weber 4 files

File Tags File Archives December 2022 Advisory (79,754) Arbitrary (15.694) October 2022 BBS (2.859) September 2022 August 2022 Bypass (1,619) CGI (1,018) July 2022 Code Execution (6,926) June 2022 Conference (673) May 2022 April 2022 Cracker (840) 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) Systems Firewall (821) AIX (426) Info Disclosure (2,660) Apple (1,926) Intrusion Detection (867) BSD (370) CentOS (55) JavaScript (821) Cisco (1.917) Kernel (6,291) Debian (6,634) Local (14,201) Magazine (586) FreeBSD (1.242) Gentoo (4.272) Perl (1.418) PHP (5.093) iOS (330) Proof of Concept (2,291) iPhone (108) Protocol (3,435) IRIX (220) Python (1.467) Juniper (67) Remote (30.044) Linux (44,315) Mac OS X (684) Ruby (594) Mandriva (3.105) Scanner (1.631) Security Tool (7,777) OpenBSD (479) Shell (3,103) RedHat (12,469) Shellcode (1,204) Slackware (941) Sniffer (886) Solaris (1,607)

Spoof (2,166) SUSE (1,444) SQL Injection (16,102) Ubuntu (8,199) TCP (2,379) UNIX (9,159) Trojan (686) UnixWare (185) UDP (876) Windows (6,511) Virus (662) Other Vulnerability (31,136) Web (9,365) Whitepaper (3,729)



x86 (946) XSS (17,494)

Site Links About Us

News by Month History & Purpose Contact Information News Tags

Files by Month Terms of Service File Tags
File Directory Privacy Statement

Copyright Information

Hosting By Rokasec

Follow us on Twitter

