CVE-2022-34009

gainsec July 27, 2022

I (Jon Gaines) was testing an open source web application called Fossil SCM to help teach a friend of mine (Tyler Fryxell) one night a few months ago and discovered a Denial of Service (DoS).

I disclosed it to the developers and submitted a CVE assignment request!

It was approved!

Here is some information I will share about the vulnerability.

I discovered it on a Fossil instance running on a Windows machines with Windows Defender running as the anti-virus. It was a fresh install but completely up to date.

The problem is was when you submit a ticket with malicious strings (I used this whole text found HERE). Although you might be able to just use an EICAR string (found HERE) I'll have to test that in the future.

Note that an anonymous user can create and submit this ticket. What happens is the application writes the ticket to a temporary file located at

```
C:\Users\USERNAME\AppData\Local\Temp\fossil_server_*
```

This results in Windows Defender flagging the file and (the application attempting to write the ticket again to a temporary file over and over again) crashing the application, making it inaccessible.

I tested it against version 2.18.

More information can be found HERE

Stay tuned as I have a bunch more new CVEs incoming!

‹ How to Find the next BIG Data Leak in under 20 minutes or less! – LeakLooker-X – Updated 2022

CVE-2022-34625 – Server-Side Template Injection to Remote Code Execution (SSTI) to (RCE) in Mealie – A lesson in patience ›

Leave a Reply

Enter your comment here...

Search …

Twitter Feed

Jon G Retweeted

Robo... · Nov 24

Replying to @GergelyOrosz

I wonder how long it'll take Twitter to develop a company culture around managing Elon.

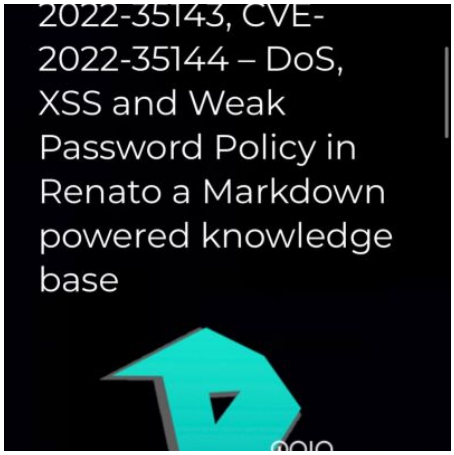
13 377

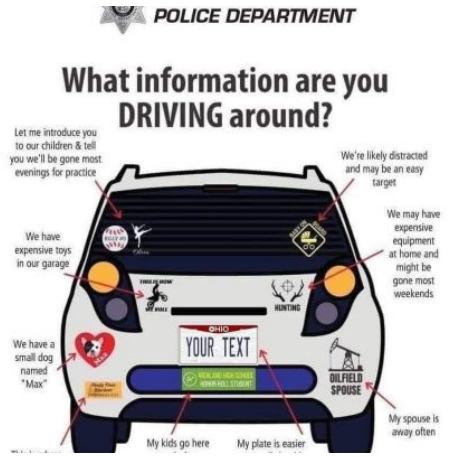
@gain_sec

Cyber Security, Privacy, Psychology, Piracy and Law

Follow on Instagram

Gain Awareness. Gain Peace of mind. Gain Security™
NO SECURITY = NO LIFE
#gainsec





Load More Posts

Follow Us