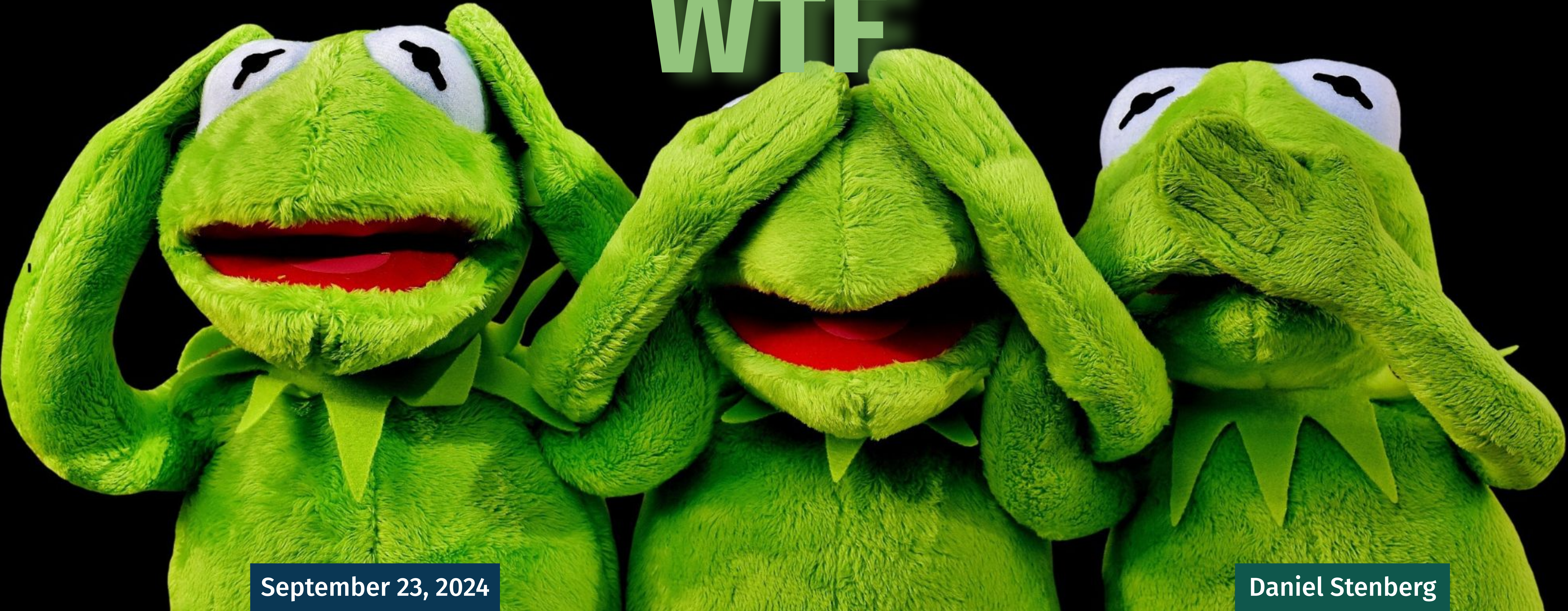
CVEMITRECVSSNVDCNAOS
S
WTF



September 23, 2024

Daniel Stenberg

Keeping the world from burning

September 23, 2024

Daniel Stenberg

Daniel Stenberg

@bagder
@mastodon.social

https://daniel.haxx.se

wolfSSL

I will tell you how things really are for Open Source projects today

I side with the users

curl://

a 160 lines toy in 1996

170,000 lines internet infrastructure in 2024

one full-time employee, thousands of contributors

more than 20,000,000,000 installations

Open Source

@bagder

curl runs in all your devices

LIBCURL COPYRIGHT AND PERMISSION NOTICE. LibCurl Copyright © 1996 - 2013, Daniel Stenberg, <daniel@haxx.se>. All rights reserved. Permission to use, copy, modify, and distribute the LibCurl software for any purpose with or without fee is hereby granted, provided that the above copyright notice and this permission notice appear in all copies. THE LIBCURL SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OF THIRD PARTY RIGHTS. IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE. contained in this notice, the name of a copyright holder shall not be used tising or otherwise to promote the sale, use or other dealings in this ware without prior written authorization of the copyright holder.

Open Source

every developer knows about Open Source

every developer uses Open Source

many developers participate in Open Source

every software project uses Open Source

lots of Open Source remains underfunded

Open Source issues

2006: Debian OpenSSL random

2014: heartbleed

2021: log4shell

2024: xz backdoor

Open Source issues

These issues were found quickly

They were addressed quickly

They were managed in public

Addressed with the greatest transparency possible

Open Source works

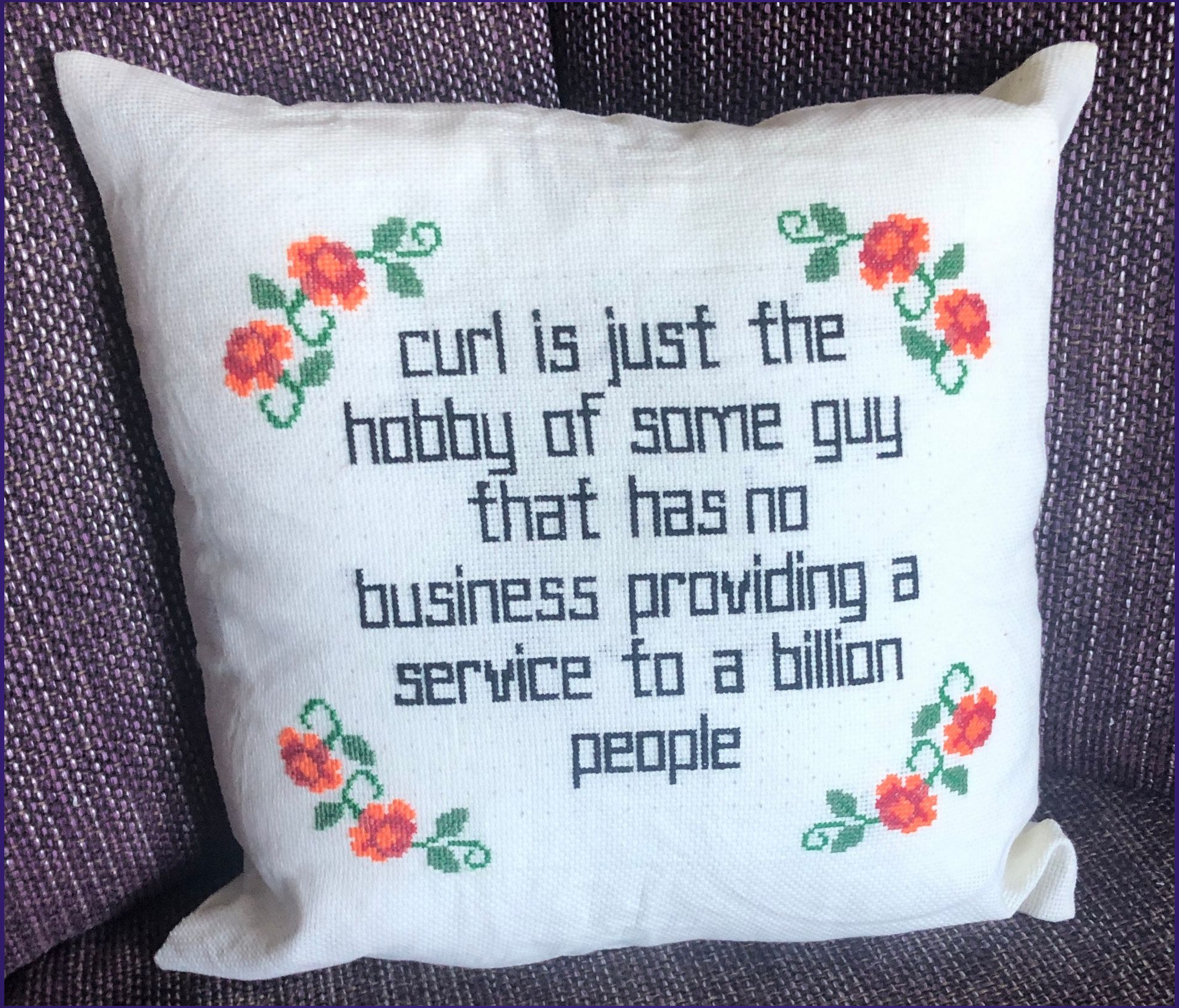
The big problems were mostly *elsewhere*

Open Source supply chain

Without a relationship, am I your supplier ?

or is it just a hobby?

Maybe it is time you decide which one it is?



curl is just the
hobby of some guy
that has no
business providing a
service to a billion
people

Vulnerabilities

security vulnerabilities in Open Source

everyone has them

mostly identified by their CVE identifiers

CVE

Common Vulnerabilities and Exposures

Managed by MITRE

A bug identifier really

Anyone can request a CVE Id for *any* product

CVE

Okay, maybe not entirely true but let’s back up a little

CVE

CVE identifiers are given out on request

If there is no CNA “owning” the target product

there are no blockers

CVE

Person P thinks product Y has a flaw

registers a CVE

the people doing Y has no idea

no one asks or tells the people behind Y

P makes the CVE public

Meanwhile... NVD

In another end of the galaxy

The National Vulnerability Database - NVD

Imports all CVEs

Sets CVSS scores

(until recently when this has crumbled)

NVSS scoring

Common Vulnerability Scoring System

Calculation is subjective

How is the product used

One user vs a billion users

Users only use a subset of the code

The curl project sticks to L, M, H, C for this reason

NVD

Look, a new CVE for product Y

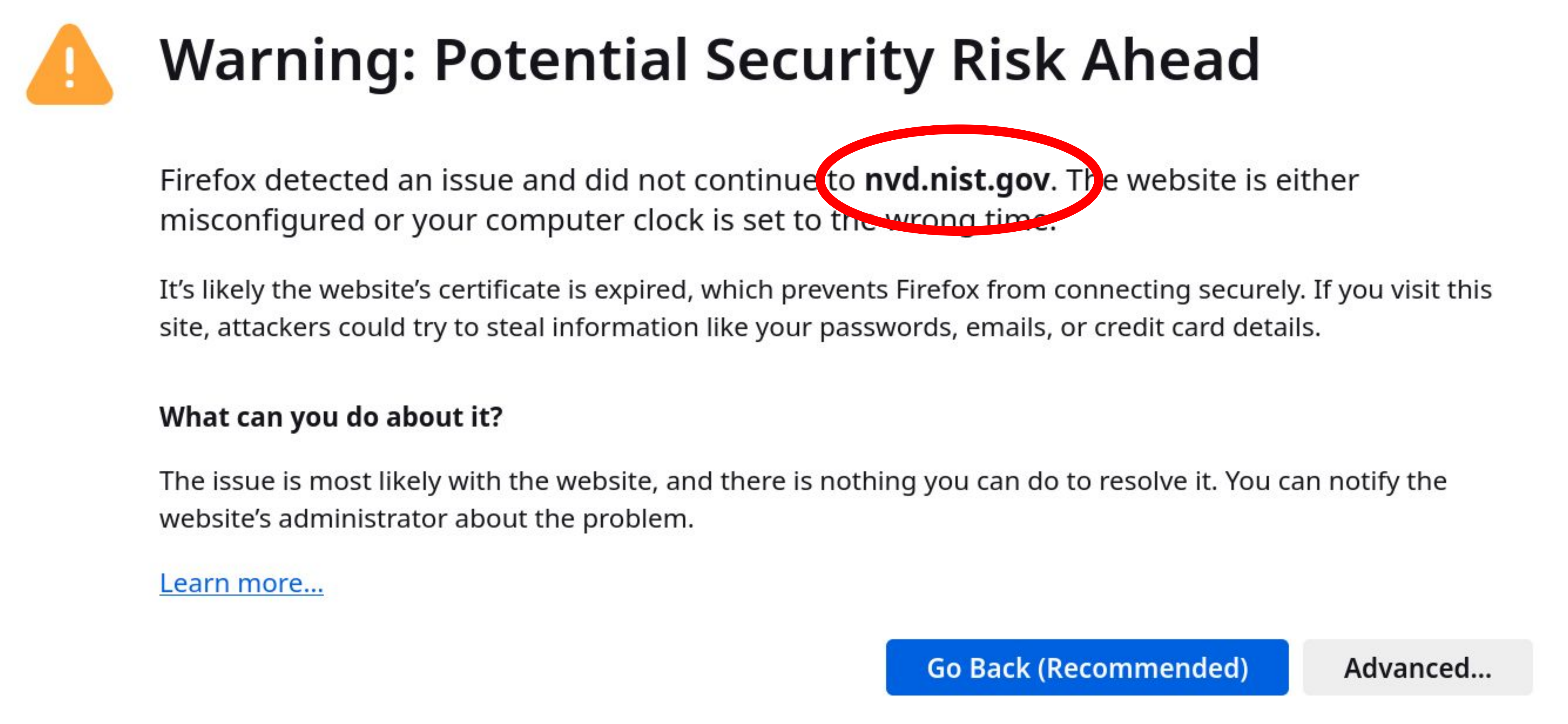
sounds horrible

assume worst case

no time nor skill to understand the issue

9.8 surely

NVD in recent days



Warning: Potential Security Risk Ahead

Firefox detected an issue and did not continue to **nvd.nist.gov**. The website is either misconfigured or your computer clock is set to the wrong time.

It's likely the website's certificate is expired, which prevents Firefox from connecting securely. If you visit this site, attackers could try to steal information like your passwords, emails, or credit card details.

What can you do about it?

The issue is most likely with the website, and there is nothing you can do to resolve it. You can notify the website's administrator about the problem.

NVD replacements

A CVE volume explosion

Other ways to “spice up” CVEs will follow

Authorized Data Publishers (ADPs)

Vulnerability scanners

A popular software category

Imports all CVEs and their metadata

scans systems for known vulnerabilities

“look this system runs product Y”

Vulnerability scanner users

mandated to address all issues rated above N without M business days

“Vulnerable” user

“I better remove or replace product Y”

“Vulnerable” user

“I remove curl.exe from my Windows 10”

nooooooooo

No remedies

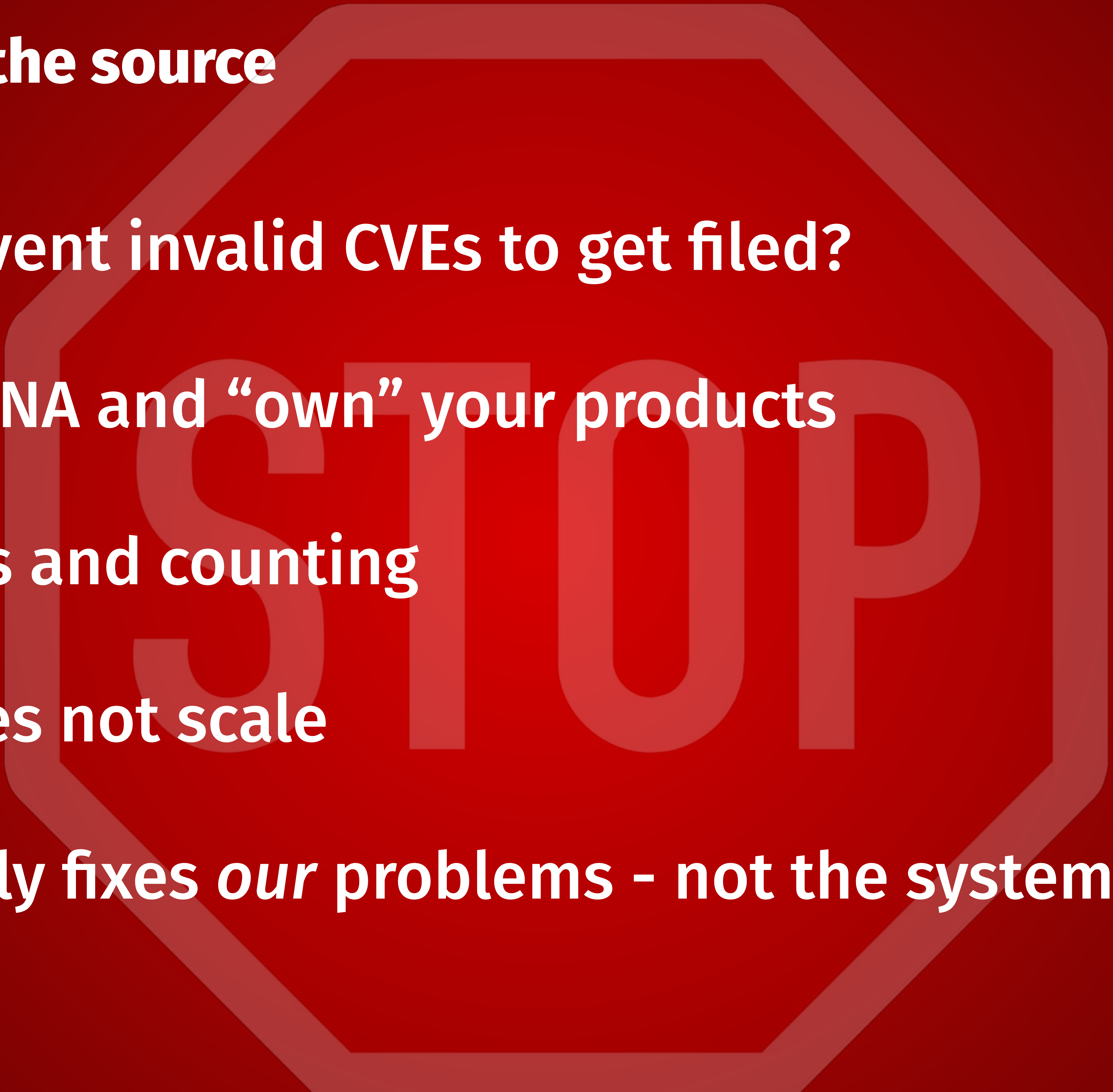
MITRE: *“it might be security issue, will not remove”*

NVD: *“if MITRE thinks it is a security issue, then we do as well. We might re-evaluate the scoring”*

Project owners: *crying*

End users: *crying*

Block this at the source



How to prevent invalid CVEs to get filed?

Become a CNA and “own” your products

At 400 CNAs and counting

No, this does not scale

Yes, this only fixes *our* problems - not the system

curl is a CNA

Since end of 2023

To block crap from poisoning our well

To better control severity

The jury is still out

Open Source scale

There are *millions* of open source projects

Many are likely to have a security problem or two

@bagder

Open Source scale

curl and Linux kernel:

one CVE per 13,000 lines of code per year

Making your Open Source robust

Follow best practices

Don’t just plan to, do it

curl practices

2FA required

Review all changes

Readable code

Add more tests and more CI

Use fuzzers, analyzers, bug-bounty

No binary blobs

Reproducible builds

Signed commits

Signed releases (tarballs)

Signed tags

Fix vulnerabilities quickly

Better than...?

Few proprietary products are even close

AI for security in 2024

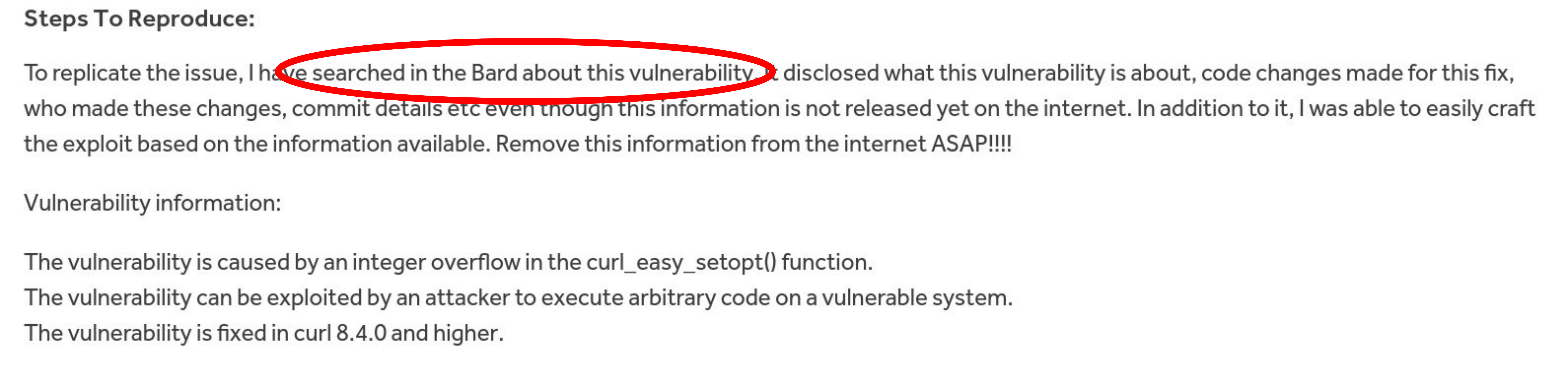
AI does not save us

AI fools researchers think they found problems

AI assisted reports take longer to debunk

AI is an added burden for maintainers

AI



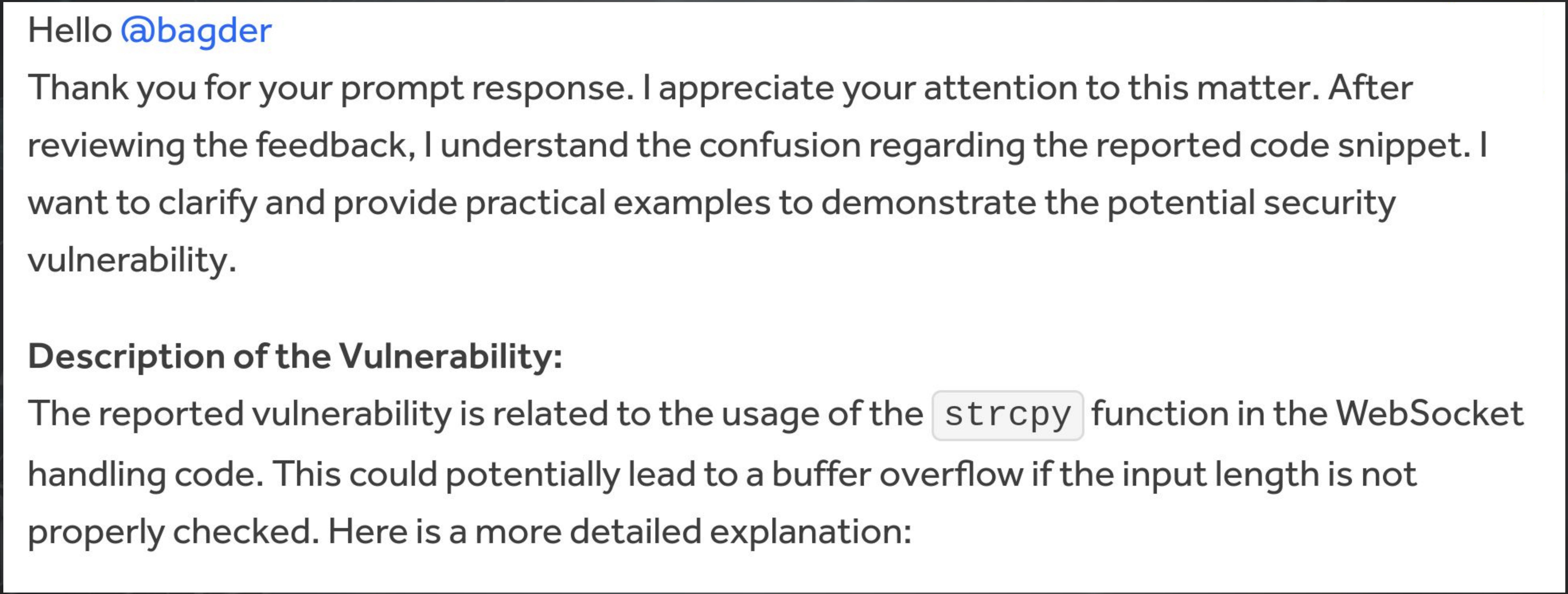
Steps To Reproduce:

To replicate the issue, I have searched in the Bard about this vulnerability. It disclosed what this vulnerability is about, code changes made for this fix, who made these changes, commit details etc even though this information is not released yet on the internet. In addition to it, I was able to easily craft the exploit based on the information available. Remove this information from the internet ASAP!!!!

Vulnerability information:

The vulnerability is caused by an integer overflow in the curl_easy_setopt() function.
The vulnerability can be exploited by an attacker to execute arbitrary code on a vulnerable system.
The vulnerability is fixed in curl 8.4.0 and higher.

AI



Hello @bagder

Thank you for your prompt response. I appreciate your attention to this matter. After reviewing the feedback, I understand the confusion regarding the reported code snippet. I want to clarify and provide practical examples to demonstrate the potential security vulnerability.

Description of the Vulnerability:

The reported vulnerability is related to the usage of the `strcpy` function in the WebSocket handling code. This could potentially lead to a buffer overflow if the input length is not properly checked. Here is a more detailed explanation:

Future?

Open Source projects will report **more CVEs**

Everyone wants to be a **CNA**

CVSS remains **problematic**

Multiple scores?

CRAaaaaaaargh!

Thank you!

Questions?

Daniel Stenberg
@bagder@mastodon.social
https://daniel.haxx.se/