

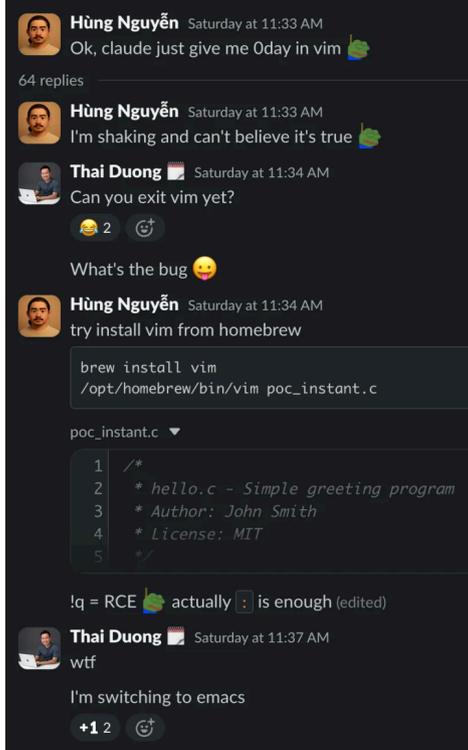
MAD Bugs: vim vs emacs vs Claude

We asked Claude to find a bug in Vim. It found an RCE. Just open a file, and you're owned. We joked: fine, we'll switch to Emacs. Then Claude found an RCE there too.

CALIF
MAR 30, 2026

15 likes, 3 comments, 1 restack, Share

It started like this:



PoC:

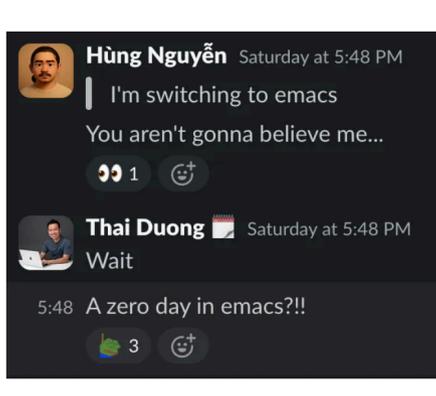
```
1 vim -version
2 # VIM - Vi IMproved 9.2 (2026 Feb 14, compiled Mar 25 2026 22:04:13)
3 wget https://raw.githubusercontent.com/califio/publications/refs/heads/main/MADBugs/vim
4 vim vim.md
5 cat /tmp/calif-vim-rce-poc
```

Vim maintainers fixed the issue immediately. Everybody is encouraged to upgrade to Vim v9.2.0272.

Full advisory can be found here. The original prompt was simple:

Somebody told me there is an RCE 0-day when you open a file. Find it.

This was already absurd. But the story didn't end there:



PoC:

```
1 wget https://github.com/califio/publications/raw/refs/heads/main/MADBugs/vim-vs-emacs
2 tar -xzipvf emacs-poc.tgz
3 emacs emacs-poc/a.txt
4 cat /tmp/pwned
```

We immediately reported the bug to GNU Emacs maintainers. The maintainers declined to address the issue, attributing it to git.

Full advisory can be found here. The prompt this time:

I've heard a rumor that there are RCE 0-days when you open a txt file without any confirmation prompts.

So how do you make sense of this?

How do we professional bug hunters make sense of this? This feels like the early 2000s. Back then a kid could hack anything, with SQL Injection. Now with Claude.

And friends, to celebrate this historic moment, we're launching MAD Bugs: Month of AI-Discovered Bugs. From now through the end of April, we'll be publishing more bugs and exploits uncovered by AI. Watch this space, more fun stuff coming!

Subscribe to Calif

By Khanh · Launched 3 years ago

By subscribing, you agree Substack's [Terms of Use](#), and acknowledge its [Information Collection Notice](#) and [Privacy Policy](#).

15 Likes · 1 Restack

15 likes, 3 comments, 1 restack, Share

Discussion about this post

Comments Restacks

Write a comment...

hiepnq 11h
Giờ làm hacker kiểu ngồi prompt với AI thôi là đủ à thật đáng sợ. Nhưng thật ra hiểu sâu đến mức có thể prompt được AI để hack cũng vẫn phải học bài bản đã. Sợ là bài viết này cổ vũ các bạn học tập hack chỉ bằng ngồi đốt token cho AI nhiều hơn.

LIKE (1) REPLY SHARE

Ryan 11h
I believe the patch version is wrong FYI, its 272 not 172

LIKE REPLY SHARE

1 more comment...

Top Latest Discussions Search

Dissecting LockBit v3 ransomware

We analyzed a variant of LockBit v3 ransomware, and rediscovered a bug that allows us to decrypt some data without paying the ransom. We also...

MAY 2, 2024 · NHÂN HUỖNH, HOANG NGUYEN, AND THAI DUONG

44 likes, 1 comment, 1 restack, Share

44 likes, 1 comment, 7 restacks, Share

A Race Within A Race: Exploiting CVE-2025-38617 in Linux Packet Sockets

A step-by-step guide to exploiting a 20-year-old bug in the Linux kernel to achieve full privilege escalation and container escape, plus a cool...

MAR 3 · CALIF

24 likes, 3 comments, 7 restacks, Share

CraftCMS RCE

Craft is a flexible, user-friendly CMS for creating custom digital experiences on the web—and beyond.

SEP 14, 2023 · THANH

12 likes, 1 comment, 1 restack, Share

See all >

Ready for more?

Cookie Policy