

Forum:[Hack Forums](#)

Thread: [20-Year-Old Radio Exploit Lets Attackers Trigger Train Brakes \[CVE-2025-1727\]](#)

JoseMar - July 16, 2025, 1:28 am

20-Year-Old Radio Exploit Lets Attackers
Trigger Train Brakes [CVE-2025-1727]

So, imagine this: You're standing near the edge of a train platform. Not doing anything dramatic, just waiting. And somewhere out there, a random person with some radio gear could, in theory, pull that train's emergency brake. Remotely.

Not because they hacked a laptop.
Not because they broke into some facility.
But because of... a 20-year-old design flaw.

That's the part that messes with me.

CISA just dropped an advisory about CVE-2025-1727, a newly exposed vulnerability in train brake communication systems that's been sitting in plain sight for two decades. It affects the remote link between the End-of-Train and Head-of-Train devices, basically the wireless handshake that tells a train it's safe to keep moving.

The protocol is called FRED. Yes, FRED. It's kind of charming, until you realize it's critically flawed.

At the core? A weak BCH checksum used for authentication. Which, for those who don't swim in this stuff daily, means the system relies on math that's really easy to fake. And if you've got a software-defined radio and some know-how, you can spoof a legit brake command.

That's it. You can stop a train.

No login, no deep exploit chain, no Mission Impossible nonsense.

Just bad design left untouched for years.

New entry for [7](#)contest?

? Big shoutout to [6](#) for making this even more exciting?

Hey guys, check this out.?

[DemonAsylum Nightmare](#) [mention=3865317] [mention=3297465] [Prettykitty skull account](#) [Money-](#)

This isn't some niche hobby railway either. We're talking about protocols used across the U.S. rail network, by major manufacturers like Siemens, Wabtec, and Hitachi.

Researchers Neil Smith and Eric Reuter figured this out (respect, honestly), and now the scramble begins: isolate the network, patch where possible, update what's ancient. But it's not that simple.

Because, let's be real, trains don't get new hardware overnight. Some of these systems are embedded. Legacy. Deeply integrated into infrastructure. Upgrading them is slow and expensive and probably involves meetings that take six months to schedule.

So what now?

CISA's doing the right thing: telling orgs to lock down access, isolate critical systems, and reach out to manufacturers. And so far, no known attacks have happened. That's the one semi-comforting part.

But still... I can't shake the weird feeling. It's not even about this one flaw. It's about how many more are still out there. Quiet vulnerabilities. Ancient protocols. Stuff built long before cybersecurity was a boardroom word.

It's easy to think of cyber risks in terms of email hacks or ransomware. But this? This is kinetic. Physical. It stops metal in motion. That makes it real in a way some zero-day in a smart fridge just... doesn't.

Anyway, I'm not here to sound the alarm like some doomsayer. Honestly, I'm just thinking out loud.

But I do think we're long overdue for a cultural shift in how we handle industrial systems. Not everything has to connect to the internet. And if it must connect, maybe we should stop pretending 20-year-old math can keep up.

The vulnerability has technically existed for decades, but only now is it being recognized as a serious security risk. Back then, this kind of system was seen as "secure enough," in an era where cyberattacks on industrial infrastructure weren't exactly common, or expected. But now? With modern tools like SDRs and rising sophistication in attacks, that once-acceptable design suddenly looks like a glaring flaw.