

CROWDSTRIKE

MORE THAN 8.5 MILLION COMPUTERS AFFECTED

5000 FLIGHTS CANCELLED BY DELTA

WORKERS IN EUROPE ACROSS BANKS, HOSPITALS, AND OTHER MAJOR INSTITUTIONS
UNABLE TO LOG IN TO THEIR SYSTEMS. AND IT QUICKLY BECAME APPARENT THAT IT WAS
ALL DUE TO ONE SMALL FILE.





TheBelerine • 6d ago

Most viewed color on 7/19/24: Blue

↑ 81 ↓ 🧐 1 ↗ Share ...



Beugie44 • 6d ago

This is what y2k wishes it was

⊖ ↑ 288 ↓ 🧐 3 ↗ Share ...



[deleted] • 6d ago • Edited 6d ago

Time to log in and check if it hit us...oh god I hope not...350k endpoints

EDIT: 210K BSODS all at 10:57 PST....and it keeps going up...this is bad....

EDIT2: Ended up being about 170k devices in total (many had multiple) but not all reported a crash (Nextthink FTW). Many came up but looks like around 16k hard down....not included the couple thousand servers that need to be manually booted into Safe mode to be fixed.

3AM and 300 people on this crit rushing to do our best...God save the slumbering support techs that have no idea what they are in for today



Berowulf • 6d ago

Wow, I'm a system admin whose vacation started 6 hours ago... My junior admin was not prepared for this

⊖ ↑ 98 ↓ 🧐 Award ↗ Share ...



Rude_Strawberry • 5d ago

My company has about 15000 devices across 20+ countries, all on different domains, 365 tenants and random shitty infrastructure dotted about the place in dodgy data centres.

I was watching the ticket queue earlier, especially when America woke up as I'm based in England. 1 new ticket every couple of seconds about a blue screen. Tickets up in the 1000s.

Majority of devices intune joined, encrypted so the fixes people provide on here just do not apply to my company.

Basically we are fecked for the next few weeks.



LForbeslam • 4d ago • Edited 4d ago

This took down ALL our Domain Controllers, Servers and all 100,000 workstations in 9 domains and EVERY hospital. We spent 36 hours changing bios to ACHI so we could get into Safemode as Raid doesn't support safemode and now we cannot change them back without reimaging.

Luckily our SCCM techs were able to create a task sequence to pull the bitlocker pwd from AD and delete the corrupted file, and so with USB keys we can boot into SCCM TS and run the fix in 3 minutes without swapping bios settings.

At the end of June, 3 weeks ago, CrowdStrike sent a corrupted definition that hung the 100,000 computers and servers at 90% CPU and took multiple 10 Minute reboots to recover.

We told them then they need to TEST their files before deploying.

Obviously the company ignored that and then intentionally didn't PS1 and PS2 test this update at all.

How can anyone trust them again? Once they make a massive error a MONTH ago and do nothing to change the testing process and then proceed to harm patients by taking down Emergency Rooms and Operating Rooms?

As a sysadmin for 35 years this is the biggest disaster to healthcare I have ever seen. The cost of recovery is astronomical. Who is going to pay for it?



BattleScones • 6d ago

Just tried to call a local news agency in New Zealand to let them know that I know how to resolve the problem and that I've tested it, the guy said "I'm only dealing with breaking news currently".

Literally 1 hour later and it's the only thing I can see on any news outlet.



WangNuts • 6d ago

Big thank you to Australia for beta testing.

↑ 14 ↓ Award Share ...

+ 7 more replies



PurchasePristine8017 • 6d ago

Damn we got E-covid

↑ 13 ↓ Award Share ...

+ 4 more replies



thechosen1s • 6d ago

International Bluescreen Day!

↑ 9 ↓ Award Share ...

+ 2 more replies



sk8hackr • 6d ago

Crowdstrike customers account for 298 of the Fortune 500...

⊖ ↑ 11 ↓ Award Share ...



elmobob • 4mo ago •

[No Title]

I work in IT for a large organization with multiple buildings spread out providing critical services in the east coast US, we have crowdstrike in every windows host, most of our servers (thousands) went down and still recovering, over 75% of our desktops blue screened with half of them stuck in the BSOD boot loop. Adding a monkey wrench to this, our desktops / laptops use a non Microsoft full disk encryption solution. It's been one hell of a ride so far. I'm part of the desktop endpoint management team and at 1:45am yesterday before we knew the issue was crowdstrike I woke up to an emergency conference call being asked if my team had deployed any windows updates or something else causing this, I could not immediately access our admin console so I was triple guessing myself thinking we did something by mistake. Adrenaline levels thru the roof..



CaptainFluffyTail • 4mo ago • Edited 4mo ago •

Being a part of history. Woooo.

Half the team is down because the laptops bugchecked and getting the bitlocker key is proving to be more difficult than anticipated.

The couple folks running Macs were laughing at first but they are doing all the work now since they have a stable device.

A WORKAROUND – TAKES TIME AND REQUIRES SNEAKER-NET

"reboot and wait" by u/Michichael comment

As of 2AM PST it appears that booting into safe mode with networking, waiting ~ 15 for crowdstrike agent to phone home and update, then rebooting normally is another viable work around.

"keyless bitlocker fix" by u/HammerSlo comment (improved and fixed formatting)

1. Cycle through BSODs until you get the recovery screen.
2. Navigate to **Troubleshoot > Advanced Options > Startup Settings**
3. Press **Restart**
4. Skip the first Bitlocker recovery key prompt by pressing **Esc**
5. Skip the second Bitlocker recovery key prompt by selecting **Skip This Drive** in the bottom right
6. Navigate to **Troubleshoot > Advanced Options > Command Prompt**
7. Type `bcdedit /set {default} safeboot minimal` . then press enter.
8. Go back to the WinRE main menu and select **Continue**.
9. It may cycle 2-3 times.
10. If you booted into safe mode, log in per normal.
11. Open Windows Explorer, navigate to `C:\Windows\System32\drivers\CrowdStrike`
12. Delete the offending file (STARTS with `C-00000291*. sys` file extension)
13. Open command prompt (as administrator)
14. Type `bcdedit /deletevalue {default} safeboot` , then press enter. 5. Restart as normal, confirm normal behavior.



thadiuswhacknamara • 6d ago

Let's say booting into safe mode and applying the "workaround" takes five minutes per host, and you have one hundred hosts, about five hundred minutes. Plus travel. Let's realistically say, for a company with 20k hosts and they're all shit out of date crap, eleven minutes per host 242 thousand minutes. Divide that by the number of techs, put that over sixty, multiply it by the hourly rate, add the costs in lost productivity and revenue. Yep - this is the most expensive outage in history so far.

PUB IS OPEN

 **Appropriate-Lab3998** • 6d ago

Why push this update on a Friday afternoon guys? why?!?!?!

  89   Award  Share ...

 **Tricky-Watercress-51** • 6d ago

They wanted to go to the pub early!

  37   Award  Share ...

 **Kurshu** • 6d ago

Unfortunately, the pub's tills also run on windows :(

 19   Award  Share ...

 **Glum-Guarantee7736** • 6d ago

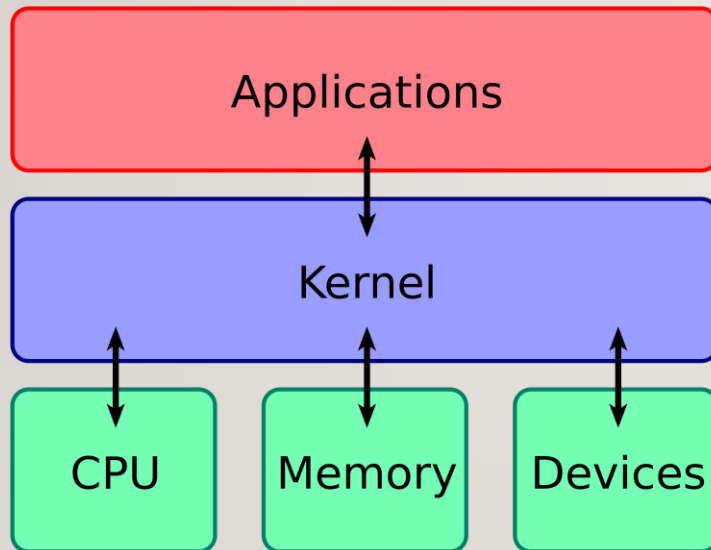
Ransomware is the single biggest threat to corp IT. Crowdstrike: hold my beer...

 20   Award  Share ...

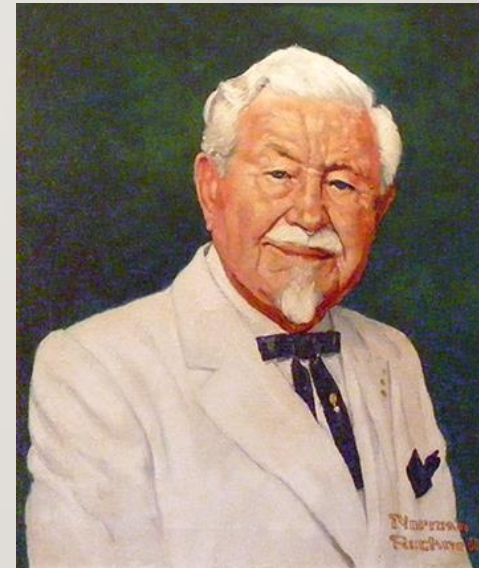
 5 more replies

WHAT CAUSED THE CHAOS?

- The Kernal gives access to memory and disk.
- The trade off here is: anything goes wrong, the system must blue screen to protect the OS, files etc.



By Bobbo - Own work, CC BY-SA 3.0, <https://commons.wikimedia.org/w/index.php?curid=4392180>



CC Image courtesy Winston L Shelton

KERNEL DRIVERS

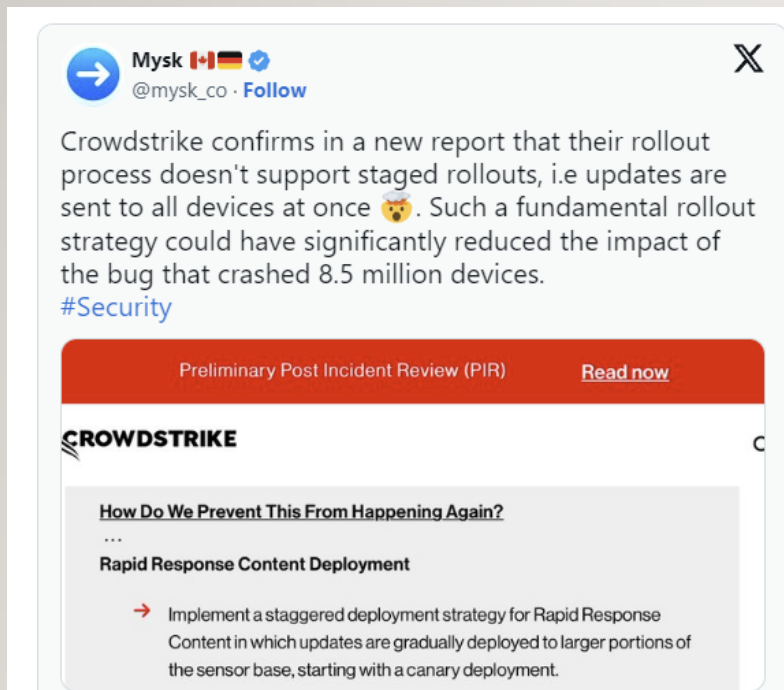
Kernel drivers also improve performance, which is why they are often used by security vendors. For example, analysis or data collection for high throughput network activity may benefit from a kernel driver, Microsoft points out.


Another benefit of loading into kernel mode is tamper resistance. “Security products want to ensure that their software cannot be disabled by malware, targeted attacks, or malicious insiders, even when those attackers have admin-level privileges,” Microsoft says. “They also want to ensure that their drivers load as early as possible so that they can observe system events at the earliest possible time.”

IN A NUTSHELL

- CrowdStrike is a kernel driver, meaning that it has access to privileged information like the OS memory map, etc
- A crash in a Kernel mode application implies a system crash because the alternative is worse (memory corruption, etc). This is not a windows only behaviour, all modern OS do it.
- Drivers are usually verified by MS but this process takes days so it's not suitable for CrowdStrike
- CrowdStrike driver (which is signed) dynamically executes non-signed code downloaded from its servers instead
- This code was probably not protected against improper behaviour, leading to a null pointer, instead of gracefully failing
- Normal drivers do not normally cause the OS to crash on boot but CrowdStrike is a boot start driver meaning the OS will refuse to load without it.
- Only recourse is to start in fail safe mode that only loads a limited set of drivers

WHAT DID CROWDSTRIKE LEARN?



Mysk 
@mysk_co · Follow

CrowdStrike confirms in a new report that their rollout process doesn't support staged rollouts, i.e updates are sent to all devices at once 🐞. Such a fundamental rollout strategy could have significantly reduced the impact of the bug that crashed 8.5 million devices.
[#Security](#)

Preliminary Post Incident Review (PIR) [Read now](#)

CROWDSTRIKE

How Do We Prevent This From Happening Again?
...

Rapid Response Content Deployment

- Implement a staggered deployment strategy for Rapid Response Content in which updates are gradually deployed to larger portions of the sensor base, starting with a canary deployment.

How CrowdStrike Will Prevent It From Happening Again

CrowdStrike has outlined a number of steps it will take to stop anything this devastating from happening again. This includes better testing processes such as “a staggered deployment strategy for Rapid Response Content in which updates are gradually deployed to larger portions of the sensor base, starting with a canary deployment.”

It will also improve monitoring for both sensor and system performance, collecting feedback during Rapid Response Content deployment to guide a phased rollout.

CrowdStrike says it will provide customers with greater control over the delivery of Rapid Response Content updates by “allowing granular selection of when and where these updates are deployed.”

THAT'S NOT A BLUE SCREEN OF DEATH

— **shockz** 2 days ago (Edited)

↳ *In reply to ncgonz*

It's also not the bitlocker recovery screen, although that one is also coming up too. This is just the standard, "your pc has failed to start several times, do you want to try something else" screen.

👍 Rec 1 ↳ Reply 🗨️ Share

🚩 Report

— **Daishi** 2 days ago

That's still not the Blue Screen of Death.

👍 Rec ↳ Reply 🗨️ Share

🚩 Report

— **apparatchiki** 2 days ago

↳ *In reply to Daishi*

I'm sure Delta will be relieved to know it's not technically a BSOD, this changes everything.

👍 Rec 3 ↳ Reply 🗨️ Share

🚩 Report

NYSE API: THE MOST EXPENSIVE SOFTWARE BUG (SO FAR)



Theodore Smith · Follow

Senior Software Engineer at PHP Experts (2012–present) · Upvoted by Thomas Smedley, PhD Communication & History, Regent University (2010) and Judith Meyer, learned 8 programming and 12 natural languages · Aug 6

On this day, exactly 12 years ago (9:30 EDT 1 Aug 2012), was the most expensive software bug ever, in both terms of dollars per second and total lost. The company managed to pare losses through the heroics of Goldman Sachs, and “only” lost \$457 million (which led to its dissolution).

Devs were tasked with porting their HFT bot to an upcoming NYSE API service that was announced to go live less than a 33 days in the future. So they started a death march sprint of 80 hour weeks. The HFT bot was written in C++. Because they didn't want to have to recompile once, the lead architect decided to keep the same exact class and method signature for their `PowerPeg::trade()` method, which was their automated testing bot that they had been using since 2003. This also meant that they did not have to update the WSDL for the clients that used the bot, either.

They ripped out the old dead code and put in the new code. Code that actually called real logic, instead of the test code, which was designed, by default, to buy the highest offer given to it.

They tested it, they wrote unit tests, everything looked good. So they decided to deploy it at 8 AM EST, 90 minutes before market open. QA testers tested it in prod, gave the all clear. Everyone was really happy. They'd done it. They'd made the tight deadline and deployed with just 90 minutes to spare...

The **PowerPeg trade method**, famously employed by Knight Trading, was a high-frequency trading (HFT) strategy designed to exploit inefficiencies in the stock market. Here's a simplified breakdown:

1. Market Maker Role: Knight acted as a market maker, which means they provided liquidity by offering to buy and sell stocks. This helped ensure smooth trading and stable prices.

2. "Pegging" Orders: The strategy involved placing buy or sell orders slightly ahead of existing market prices. For example, if a stock was trading at \$10.00, Knight might place an order to buy at \$10.01 or sell at \$9.99, essentially "pegging" their price near the current market price.

3. Profiting from Small Price Changes: By constantly adjusting their orders and taking advantage of tiny price fluctuations, Knight could buy low and sell high (or vice versa) in rapid succession. Each trade might yield only a small profit, but because they executed thousands of trades per second, the profits added up.

4. Speed is Key: The success of the PowerPeg method relied on advanced technology and algorithms. Knight used ultra-fast systems to analyze market data and react instantly to price movements.

5. Market Dynamics: This approach also involved analyzing how other traders were likely to behave. For example, if they detected a large order from another trader that might push prices up, Knight could adjust their strategy to profit from the anticipated movement.



They immediately went to a sprint standup and then sprint retro meeting. Per their office policy, they left their phones (on mute) at their desks.

During the retro, the markets opened at 9:30 EDT, and the new bot went WILD (!!) It just started buying the highest offer offered for all of the stocks in its buy list. The markets didn't react very abnormally, because it just looked like they were bullish. But they were buying about \$5 million shares per second... Within 2 minutes, the warning alarms were going on in their internal banking sector... a huge percentage of their \$2.5 billion in operating cash was being depleted, and fast!

So many people tried to contact the devs, but they were in a remote office in Hoboken due to the high price of real estate in Manhattan. And their phones were off and no one was at their computer.

The CEO was seen getting people to run through the halls of the building, yelling, and finally the devs noticed. 11 minutes had gone by and the bots had bought over \$3 billion of stock. The total cash reserves were depleted. The company was in SERIOUS trouble...

None of the devs could find the source of the bug. The CEO, desperate, asked for solutions. "KILL THE SERVERS!!" one of the devs shouted!!

They got techs @ the datacenter next to the NYSE building to find all 8 servers that ran the bots and DESTROYED them with fireaxes. Just ripping the wires out... And finally, after 37 minutes, the bots stopped trading. Total paper loss: \$10.8 billion.

The SEC + NYSE refused to rewind the trades for all but 6 stocks, the on paper losses were still at \$8 billion. No way they could pay. Goldman Sachs stepped in and offered to buy all the stocks @ a for-profit price of \$457 million, which they agreed to. All in all, the company lost close to \$500 million and all of its corporate clients left, and it went out of business a few weeks later.

Now what was the cause of the bug? Fat fingering human error during release.

The sysop had declined to implement CI/CD, which was still in its infancy, probably because that was his full-time job and he was making like \$300,000 in 2012 dollars (\$500k today). There were 8 servers that housed the bot and a few clients on the same servers.

The sysop had correctly typed out and pasted the correct rsync commands to get the new C++ binary onto the servers, except for server 5 of 8. In the 5th instance, he had an extra 5 in the server name. The rsync failed, but because he pasted all of the commands at once, he didn't notice...

Because the code used the exact same method signature for the trade() method, server 5 was happy to buy up the most expensive offer it was given, because it was running the Sad Path test trading software. If they had changed the method signature, it wouldn't have run and the bug wouldn't have happened.

At 9:43 EDT, the devs decided collectively to do a "rollback" to the previous release. This was the worst possible mistake, because they added in the Power Peg dead code to the other 7 servers, causing the problems to grow exponentially. Although, it took about 3 minutes for anyone in Finance to actually inform them. At that point, more than \$50 million dollars per second was being lost due to the bug.

It wasn't until 9:58 EDT that the servers had all been destroyed that the trading stopped.

Here is a description of the aftermath:

It was not until 9:58 a.m. that Knight engineers identified the root cause and shut down SMARS on all the servers; however, the damage had been done. Knight had executed over 4 million trades in 154 stocks totaling more than 397 million shares; it assumed a net long position in 80 stocks of approximately \$3.5 billion as well as a net short position in 74 stocks of approximately \$3.15 billion.

28 minutes. \$8.65 billion inappropriately purchased. ~1680 seconds. \$5.18 million/second.

But after the rollback at 9:43, about \$4.4 billion was lost. ~900 seconds. ~\$49 million/second.

That was the story of how a bad software decision and fat-fingered manual production release destroyed the most profitable stock trading firm of the time, and was the most expensive software bug in human history.

THERAC-25

- The Therac-25 was a radiation therapy machine developed in the 1980s.
- Its purpose: to treat cancer patients with high-precision radiation therapy.
- Outcome: Overdoses of radiation due to software flaws caused six deaths and severe injuries.



Image credit: Hackaday

BACKGROUND

- Previous models were mostly hardware based.
- During this era, it was thought that software could not fail.
- A sole hobbyist programmer worked on the software for the Therac-25. He left in 1986 and his identity remains unknown.
- In March, 1983, AECL performs a safety analysis of Therac-25 which apparently excluded an analysis of software.

The Therac-25 had been at the East Texas Cancer Center (ETCC) for two years before the first serious accident, and more than 500 patients had been treated. On March 21, 1986, a male patient came into ETCC for his ninth treatment on the Therac-25, one of a series prescribed as followup to the removal of a tumor from his back.

This treatment was to be a 22 MeV electron beam treatment of 180 rads on the upper back and a little to the left of his spine, for a total of 6,000 rads over six and a half weeks. He was taken into the treatment room and placed face down on the treatment table. The operator then left the treatment room, closed the door, and sat at the control terminal.

The operator had held this job for some time, and her typing efficiency had increased with experience. She could quickly enter prescription data and change it conveniently with the Therac's editing features. She entered the patient's prescription data quickly, then noticed that she had typed "x" (for X-ray) when she had intended "e" (for electron) mode. This was a common mistake as most of the treatments involved X-rays, and she had gotten used to typing this. The mistake was easy to fix; she merely used the ⤴ key to edit the mode entry.

Because the other parameters she had entered were correct, she hit the return key several times and left their values unchanged. She reached the bottom of the screen, where it was indicated that the parameters had been VERIFIED and the terminal displayed BEAM READY, as expected. She hit the one-key command, ⓑ for *beam on*, to begin the treatment. After a moment, the machine shut down and the console displayed the message MALFUNCTION 54. The machine also displayed a TREATMENT PAUSE, indicating a problem of low priority. The sheet on the side of the machine explained that this malfunction was a “dose input 2” error. The ETCC did not have any other information available in its instruction manual or other Therac-25 documentation to explain the meaning of MALFUNCTION 54. An AECL technician later testified that “dose input 2” meant that a dose had been delivered that was either too high or too low. The messages had been expected to be used only during internal company development.

The machine showed a substantial underdose on its dose monitor display—6 monitor units delivered whereas the operator had requested 202 monitor units. She was accustomed to the quirks of the machine, which would frequently stop or delay treatment; in the past, the only consequences had been inconvenience. She immediately took the normal action when the machine

merely paused, which was to hit the (P) key to proceed with the treatment. The machine promptly shut down with the same MALFUNCTION 54 error and the same underdose shown by the dosimetry.

The operator was isolated from the patient, since the machine apparatus was inside a shielded room of its own. The only way that the operator could be alerted to patient difficulty was through audio and video monitors. On this day, the video display was unplugged and the audio monitor was broken.

After the first attempt to treat him, the patient said that he felt as if he had received an electric shock or that someone had poured hot coffee on his back: He felt a thump and heat and heard a buzzing sound from the equipment. Since this was his ninth treatment, he knew that this was not normal. He began to get up from the treatment table to go for help. It was at this moment that the operator hit the (P) key to proceed with the treatment. The patient said that he felt like his arm was being shocked by electricity and that his hand was leaving his body. He went to the treatment room door and pounded on it. The operator was shocked and immediately opened the door for him. He appeared visibly shaken and upset.

The patient was immediately examined by a physician, who observed intense reddening of the treatment area, but suspected nothing more serious than electric shock. The patient was discharged and sent home with instructions to return if he suffered any further reactions. The hospital physicist was called in, and he found the machine calibration within specifications. The meaning of the malfunction message was not understood. The machine was then used to treat patients for the rest of the day.

STOP MAKING THESE CLAIMS

- After a patient complained of being burnt, they were told it was impossible.
- A second physicist viewed the patient a couple of weeks later and advised:“That looks like the exit dose made by an electron beam”.
- It didn't look like 200 rads. It was later estimated to be more like 20,000 rads (which is hundreds of times great than what you would experience if you were standing in a failed reactor at Fukushima).
- The physicist contacted a professional organization to explain what happened.
- He was later contacted by the AECL and told to “Stop making these claims”.

ITS KINDA THE SAME AS BEFORE

- Before release of Therac-25 on the US market, AECL obtained approval to market it from the FDA.
- This approval was obtained by declaring what FDA called pre-market equivalence.
- Since the software was based on software already in use, and the linear accelerator was a minor modification of existing technology, designation of Therac-25 as equivalent to this earlier technology meant that Therac-25 bypassed the rigorous FDA testing procedures.
- In 1984, 94% of medical devices entered the market in this manner.

INVESTIGATION

- Fritz Hager, the staff physicist at the East Texas Cancer Center in Tyler, Texas was instrumental in turning things around here.
- After the second incident at his facility, he was determined to get to the bottom of the problem. In both cases, the Therac-25 displayed a “Malfunction 54” message. The message was not mentioned in any documentation.
- AECL explained that Malfunction 54 meant that the Therac-25’s computer could not determine if there was an underdose OR overdose of radiation.

FINALLY – SOME TESTING

- The same radiotherapy technician had been involved in both incidents, so Fritz brought her back into the control room to attempt to recreate the problem.
- The two worked through the night and into the weekend trying to reproduce the problem. With the technician running the machine, the two were able to pinpoint the issue.
- The VT-100 console used to enter Therac-25 prescriptions allowed cursor movement via cursor up and down keys. If the user selected X-ray mode, the machine would begin setting up the machine for high-powered X-rays. This process took about 8 seconds. If the user switched to Electron mode within those 8 seconds, the turntable would not switch over to the correct position, leaving the turntable in an unknown state.



PATIENT NAME: John
TREATMENT MODE: FIX BEAM TYPE: E ENERGY (KeV): 10

	ACTUAL	PRESCRIBED	
UNIT RATE/MINUTE	0.000000	0.000000	
MONITOR UNITS	200.000000	200.000000	
TIME (MIN)	0.270000	0.270000	
GANTRY ROTATION (DEG)	0.000000	0.000000	VERIFIED
COLLIMATOR ROTATION (DEG)	359.200000	359.200000	VERIFIED
COLLIMATOR X (CM)	14.200000	14.200000	VERIFIED
COLLIMATOR Y (CM)	27.200000	27.200000	VERIFIED
WEDGE NUMBER	1.000000	1.000000	VERIFIED
ACCESSORY NUMBER	0.000000	0.000000	VERIFIED

DATE: 2012-04-16	SYSTEM: BEAM READY	OP.MODE: TREAT	AUTO
TIME: 11:48:58	TREAT: TREAT PAUSE	X-RAY	173777
OPR ID: 033-tfs3p	REASON: OPERATOR	COMMAND: █	

TRIPPING THE FUSE

- Frank Borger, staff physicist for a cancer center in Chicago proved that the bug also existed in the Therac-20's software.
- By performing Fritz's procedure on his older machine, he received similar error, and a fuse in the machine would blow.
- The fuse was part of a hardware interlock which had been removed in the Therac-25.

- 1988 AECL dissolved their medical equipment department and settled law suits.

REFERENCES

- <https://ethicsunwrapped.utexas.edu/case-study/therac-25>
- <https://www.cs.columbia.edu/~junfeng/08fa-e6998/sched/readings/therac25.pdf>
- https://www.reddit.com/r/crowdstrike/comments/1e6vmkf/bsod_error_in_latest_crowdsstrike_update/
- <https://www.crowdstrike.com/en-us/blog/falcon-content-update-preliminary-post-incident-report/>