# Here's how a hacker set off Dallas' emergency sirens last weekend

By Written by Zack Whittaker, ContributorContributor April 12, 2017 at 2:05 p.m. PT

Archived: 2026-04-05 20:04:01 UTC

(Image: file photo)

During the weekend, a hacker activated Dallas' emergency outdoor sirens, which are designed to warn local residents in the event of a tornado or severe weather. Officials said at first it was a system malfunction, but then they said it was a "hack."

Now, with more details coming to light, researchers think they know how the unknown hacker pulled it off.

**Security**

- 
- 
- 
- 

At a press conference on Monday, Dallas city manager T. C. Broadnax confirmed at a press conference the intrusion that caused the sirens to go off around the city was a "radio issue" that is used to centrally control the siren system, rather than an issue with the computer system -- effectively ruling out one of the various theories that an attacker had remotely logged in with a stolen city staff password.

Broadnax wouldn't go into detail in an effort to prevent a similar attack, but another report, citing a city spokesperson, said that the radio had not set the system to use an encrypted signal.

In other words, it's possible that the attacker may have picked up the siren-sounding signal and broadcast it themselves.

Here's how: The city's outdoor warning system is manufactured and sold by Federal Signal, which is made up of 156 sirens placed around the city of Dallas. It's known as a hybrid system of both old and new technologies, say researchers, but they're typically controlled by a number of means, such as Dual-Tone Multi-Frequency (DTMF), for example, which can be broadcast from a central computer console over an emergency radio frequency. The Federal Communications Commission (FCC) currently has the 700MHz range reserved for US public safety.

In Dallas' case, there are a number of ways that the attack could have been carried out, but the most likely is that someone carried out a "radio replay" attack, which involves recording the radio signal that was broadcast during the latest monthly test of the emergency siren system and playing it back repeatedly on Friday, according to Bastille, a security firm specializing in finding and remediating radio frequency vulnerabilities.

That would have triggered all of the sirens at once, making the replay attack more likely than other hypotheses.

"Such a replay attack could be accomplished with a software defined radio (SDR) or with other off-the-shelf radio frequency (RF) test equipment," said Chris Risley, Bastille's chief executive.

The attack would have required someone with a deeper knowledge of radio frequencies and equipment, and they would needed to have done their homework.

"A system like the one in Dallas is typically complex, and would require someone with intimate knowledge of the frequencies, codes, and layouts pertaining to the sirens," said Kyle Wilhoit, senior security researcher at DomainTools.

"Since not all sirens may communicate in a multicast fashion, the attackers had to orchestrate this attack with excellent timing," he said.


dallas.jpg

(Image: Dallas City Hall)

Mark Loveless, a senior security researcher at Duo Labs, came to a similar conclusion. He said that most of the information needed to carry out this kind of attack can be easily found from online documentation.

"Most of this knowledge could be gleaned from Google searches, you can download manuals for a lot of different sirens and systems, and most of the software being sold to control these systems can be downloaded for free (demo versions only) allowing for a crash course in [outdoor warning system] management," said Loveless in a blog post.

We found through our own searches documentation of Federal Signal equipment, including in one case a device that is designed to send the siren-starting signals to the radios being sold with default user credentials. Any of

those devices still running default credentials could be at risk, and many of these devices are connected to the internet. It's not known, however, if Dallas' systems are internet-connected.

For now, things are over for Dallas, and lessons have been learned. Rocky Vaz, the city's director of Office of Emergency Management, said Monday that the siren system had been restored.

As for Federal Signal, the company said in an emailed statement on Monday that while it was no longer contracted to maintain Dallas' emergency outdoor sirens, the company is "actively working" with the city to find the cause of the activation.

The results of that investigation could prove useful, given that other cities may be vulnerable to similar attacks, said Risley.

"Radio frequency attacks are getting much more common as attackers can buy commercial software defined radios," he said. "Systems which use radio controls (not just Emergency Siren Systems) are often vulnerable to invisible radio attacks."

In this case, the city still doesn't seem to know who is to blame, though experts say it's not impossible to triangulate where the signal came from. The city has already called in experts at the Federal Communications Commission to help find the culprit. But, so far, the blame is on the city for not protecting the siren-activating signal in the first place.

The reality is that infrastructure and emergency systems will always be a target for hackers, and the Dallas siren attack is further evidence that even the most unassuming systems can still be attacked.

It certainly got Dallas' attention. Which city will it be next?

**VIDEO: Russian Fancy Bear hackers steal athletes' medical records**

**ZDNET INVESTIGATIONS**

---