What's an Eight Sleep?

A little while ago I asked my infosec Twitter followers what IoT device in my house they thought I found a live AWS key in.

(For those that don't know, Amazon keys can be incredibly dangerous if exposed)

Guesses ranged from a **refrigerator** to a **bidet**, but **no one got it right**.

The right answer was my **bed**.

```
stream_name = "production-eight-os-logs"
region = "us-east-1"
partition_key_field = "_BOOT_ID"
compression = "none"
healthcheck.enable = false
request.retry_max_duration_secs = 300
buffer.type = "disk"
buffer.max_size = 268435488

  [sinks.kinesis.auth]
  access_key_id = "AKIAWZMBBODM4LCTNLPM"
  secret_access_key = "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"
```

I also found a backdoor into my bed, but more on that later.

Security professionals are, in my experience, exhausted of things being connected to the internet that don't need to be. Tired of their stove, car, washing machine, and bed all being internet connected.

We want the features of the future, without sacrificing our data privacy, cybersecurity, reliability and integrity.

I want the features of a temperature controlled bed, without having to worry about random engineers and hackers giving themselves access to my bed 24/7.

Eight Sleep offered the features of temperature control: set the bed to any temperature hot or cold. For someone who suffers from insomnia this seemed worth a shot.

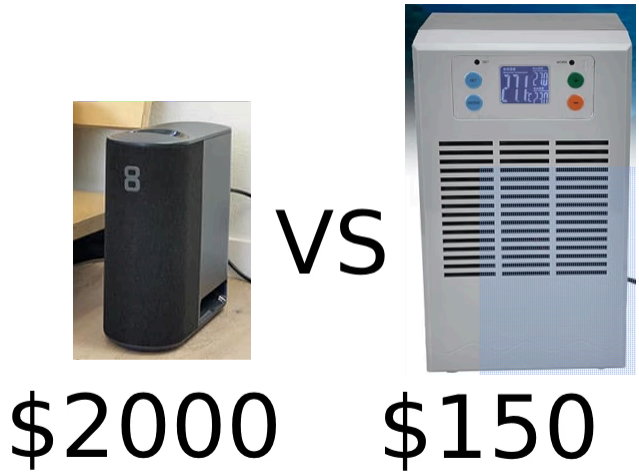
I was willing to overlook:

- The bed costs $2,000
- It won't function if the internet goes down
- Basic features are behind an additional $19/mo subscription
- The bed's only controls are via mobile app

I will say, being able to control the temperature of your bed is actually a magical thing, but after a few months, curiosity got the better of me and I took a look at the firmware.

In the end, I got enough of the cyber ick, I decided to seek a simpler, less internet-connected solution to my temperature-controlled bed needs.

It turns out inexpensive **Aquarium Chillers** provide a similar functionality as the Eight Sleep pod, without the existential dread of being hacked, and having my sleep preferences shared with a bunch of developers.



While the Eight Sleep CEO Matteo seems focused on providing DOGE with great sleep, the real doge (pictured above), whose name is Latte, is sleeping great tonight.

Stick around until the bottom of the post for how to set this up (it's easier than you think)

So let's talk about that backdoor

First of all, how did I get the bed's firmware? Easy. You can download it. Eight Sleep provides access to the firmware through their update URL:

https://update-api.8slp.net/v1/updates/p1/1?deviceId={anynumber}&currentRev=1

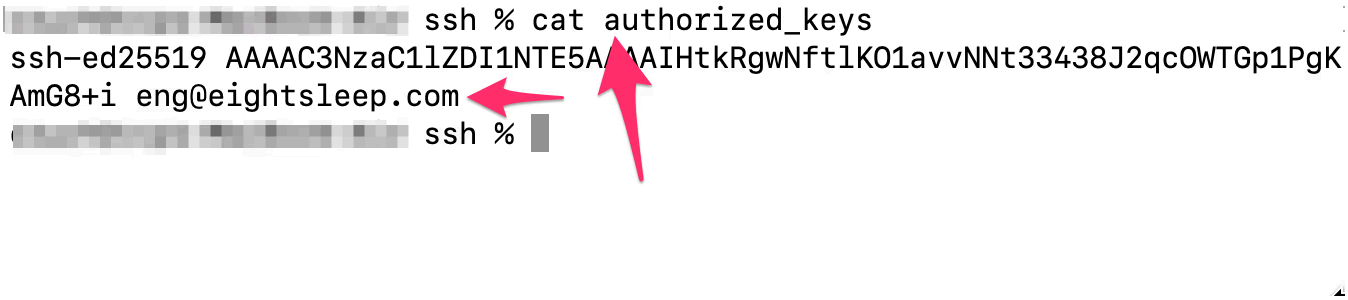
(Just replace {anynumbers} with any number)

When I say backdoor, what am I referring to? Sure, Eight Sleep needs a way to push updates, provide service, and offer support. That's expected.

What goes too far in my opinion, is **allowing all of Eight Sleep's engineers to remotely SSH into every customer's bed and run arbitrary code** that bypasses all forms of formal code review process.

And yes, I found evidence that this is exactly what's happening.

```
[redacted] % cat ./opt/eight/config/production.json
{
  "logging": {
    "name": "capybara",
    "minimumLevel": "info"
  },
  "ssh": {
    "endpoint": "remote-connectivity-api.8slp.net"
  },
  "connections": {
    "deviceAPI": "wss://device-api-ws.8slp.net/v1/device"
  }
}
```



Let's break down what's shown above. In the first image, we see evidence SSH is being exposed remotely, to a far away host, remote-connectivity-api.8slp.net. Typically SSH would only be accessible to the local area network, but the variables in production.json would seem to imply this access was opened up to a remote host.

In the second screenshot, we have the public key that's authorized to access the device. The email address attached to the public key, eng@eightsleep.com, to me suggests the private key is likely accessible to the entire engineering team.

What does this mean, exactly? Well, each bed contains a full Linux-based computer. If my estimations above are correct, all of Eight Sleep engineering can take full control of that computer any time they want.

What Can They Do with This Access?

Let's start with the basics:

- They can know when you sleep
- They can detect when there are 2 people sleeping in the bed instead of 1
- They can know when it's night, and no people are in the bed

Imagine your ex works for Eight Sleep. Or imagine they want to know when you're not home.

(Of course, they can also change the bed's temperature, turn on the vibrating feature, turn off your alarm clock, and any of the other normal controls they have power over.)

Beyond the basics, what does access to a device on your home network grant them? Any other device connected to that home network - smart fridges, smart stoves, smart washing machines, laptops - is typically routable via your bed. The (in)security of those devices is now entrusted to random Eight Sleep engineers.

Remember when Uber got in trouble for that God Mode app a few years ago? If my assumptions are correct about SSH remote access, this is in that ballpark.

The devices don't contain logs or notifications we can access to find when this is occurring.

It's possible Eight Sleep borrowed a page from Tesla.

But it should go without saying, giving engineers arbitrary SSH access on all customer devices is not best practice.

Personally, I don't want my bed data accessible to anyone, but the eight sleep sure does harvest people's bed data, and occasionally tweet about how they're watching you sleep

The key to a bad night sleep was AWS.

Well the AWS key seemed to be streaming data directly into Amazon. Of course the million dollar question is what's the policy on that key? The key could be the most dangerous thing described so far, or it could be useful for just a bit of mischief (if nothing else someone could use it to rack up a huge AWS bill for Eight Sleep)

Unfortunately, we'll never know, because as soon as I reported it, Eight Sleep revoked the key. We can tell from the surrounding context that the key had write access to Kenises, but beyond that, it's unclear.

What we do know though, is an attacker could have used that key to send 5,000 `PUT` requests per second into Kinesis and racked up a $100,000 per month bill for Eight Sleep.

Unexpected monthly bills cost us all some lost sleep.

r/EightSleep • 2 yr. ago
thebearonthatflag MOD

BUYER BEWARE - Eight Sleep has now moved basic functionality behind the paywall

Eight Sleep Shady Shit

Be aware as of February 2023 that Eight Sleep has now moved even basic functionality previously available for free like scheduling behind a monthly paywall (8+ Pro) in the app.

This includes not just previously free and now paid features like "autopilot", but now just the ability to schedule the temperature to different intervals throughout the night. You now have to pay monthly for scheduling, vibration alarm, sleep tracking, and (the pretty useless) autopilot.

So what was that about an aquarium chiller?

This process was a lot simpler than I originally imagined. Essentially all you need to do is unplug the rubber tubing from the Eight Sleep cover, which is available on eBay for a few hundred bucks, and plug it into a $150 aquarium chiller.

Eight Sleep Pod 3 Cover - Full Size (Hub NOT included) TESTED

Pre-Owned

$291.00

Buy It Now

+$83.57 delivery

travelandwork (3,800) 100%

Eight Sleep Pod 4 Cover

Pre-Owned

$400.00

or Best Offer

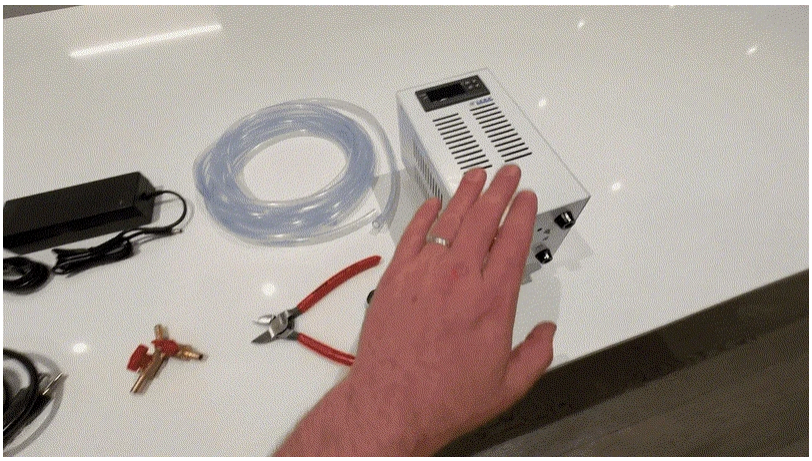
+$38.73 delivery

ri_7107 (0) 0%

There's some zip ties securing the tubes you have to cut, but other than that, it's a totally reversible, non-destructive process that takes 30 seconds.

That's it. Aquarium chillers are somewhat of a misnomer, as they can also provide heat. They use thermoelectric devices to regulate temperature, either cooling or warming the liquid that flows through them, which is the same technology found in eight sleep.

Here's a short clip of the entire process:



And now you have all the temperature control of an Eight Sleep with none of the apps, subscriptions, internet connectivity, backdoors, and security liabilities of an Eight Sleep.

There are other projects that remove the internet connectivity of the Eight Sleep, such as the Free Sleep project, but for me, I prefer the less sophisticated, physical tactile buttons of the aquarium chiller.

So what have we learned from all this?

Honestly, Eight Sleep is clearly onto something, having raised $110 million dollars in venture capital, exceeding $300 million dollars in annual revenue, ~~forcing~~ welcoming users into a subscription ~~hell~~ model, and adding to the ever growing list of devices that will one day stop working when the parent company turns their servers off.

I for one, am going to be sleeping well tonight to the warm silent circulation of an aquarium chiller, as will the Doge, Latte.