Exposed Servers Let Hackers Take Control Of Prison Cell Doors, Pacemakers, Oil Pipelines

If millions of servers, routers, switchers and personal computers are wide-open to individual hackers, how much more to rogue governments or intelligence agencies? TN Editor

Lucas Lundgren sat at his desk as he watched prison cell doors hundreds of miles away from him opening and closing.

He could see the various commands floating across his screen in unencrypted plain text. “I could even issue commands like, ‘all cell blocks open’,” he said in a phone call last week. Without being there, he couldn’t know for sure if his actions would’ve had real-world consequences.

“I’d probably only know by reading about it in the newspaper the next day,” said Lundgren, a senior security consultant at IOActive, ahead of his Black Hat talk in Las Vegas last week.

It’s because those cell doors are controlled by a little-known but popular open-source messaging protocol known as MQTT, which lets low powered, internet-connected (IoT) sensors and smart devices communicate with a central server using little bandwidth — letting prison guards remotely control the locks on a cell door. The protocol is used everywhere — by hobbyists at home, but also in industrial systems like gauges and equipment sensors, electronic billboards, and even medical devices.

But all too often, the servers that listen to devices and send commands aren’t protected with a username or password, allowing anyone with an internet connection to look into one of the 87,000 unprotected servers, according to Lundgren’s port scans.

“It’s a scary situation,” he said. “Not only can we read the data — that’s bad enough — but we can also write to the data.”

Lundgren has seen heart monitors and insulin pumps that are constantly updating data over the protocol so that a doctor can read it remotely on a web page and make alterations, he said. “If I wanted to be malicious, I could probably change the insulin or something, and see what happens,” he said.

Throughout his scans, he found servers from all over the world, running everything from home automation and alarm systems, to nuclear power plants, a particle accelerator — and even an oil pipeline.

Read full story here…