Millions of smart devices vulnerable to hacking

Researchers at a cybersecurity firm say they have identified vulnerabilities in software widely used by millions of connected devices — flaws that could be exploited by hackers to penetrate business and home computer networks and disrupt them.

By Frank Bajak

DECEMBER 8, 2020 — 8:22PM

BOSTON — Researchers at a cybersecurity firm say they have identified vulnerabilities in software widely used by millions of connected devices — flaws that could be exploited by hackers to penetrate business and home computer networks and disrupt them.

There is no evidence of any intrusions that made use of these vulnerabilities. But their existence in data-communications software central to internet-connected devices prompted the U.S. Cybersecurity and Infrastructure Security Agency to flag the issue in an advisory.

Potentially affected devices from an estimated 150 manufacturers range from networked thermometers to "smart" plugs and printers to office routers and healthcare appliances to components of industrial control systems, the cybersecurity firm Forescout Technologies said in a report released Tuesday. Most affected are consumer devices including remote-controlled temperature sensors and cameras, it said.

In the worst case, control systems that drive "critical services to society" such as water, power and automated building management could be crippled, said Awais Rashid, a computer scientist at Bristol University in Britain who reviewed the Forescout findings.

In its advisory, CISA recommended defensive measures to minimize the risk of hacking. In particular, it said industrial control systems should not be accessible from the internet and should be isolated from corporate networks.

The discovery highlights the dangers that cybersecurity experts often find in internet-linked appliances designed without much attention to security. Sloppy programming by developers is the main issue in this case, Rashid said.

Addressing the problems, estimated to afflict millions of devices, is particularly complicated because they reside in so-called open-source software, code freely distributed for use and further modification. In this case, the issue involves fundamental internet software that manages communications via a technology called TCP/IP.

Fixing the vulnerabilities in impacted devices is particularly complicated because open-source software isn't owned by anyone, said Elisa Costante, Forescout's vice president of research. Such code is often maintained by volunteers. Some of the vulnerable TCP/IP code is two decades old; some of it is no longer supported, Costante added.

It is up to the device manufacturers themselves to patch the flaws and some may not bother given the time and expense required, she said. Some of the compromised code is embedded in a component from a supplier — and if no one documented that, no one may even know it's there.

"The biggest challenge comes in finding out what you've got," Rashid said.

If unfixed, the vulnerabilities could leave corporate networks open to crippling denial-of-service attacks, ransomware delivery or malware that hijacks devices and enlists them in zombie botnets, the researchers said. With so many people working from home during the pandemic, home networks could be compromised and used as channels into corporate networks through remote-access connections.

Forescout notified as many vendors as it could about the vulnerabilities, which it dubbed AMNESIA:33. But it was impossible to identify all affected devices, Costante said. The company also alerted U.S., German and Japanese computer security authorities, she said.

The company discovered the vulnerabilities in what it called the largest study ever on the security of TCP/IP software, a year-long effort it called Project Memoria.