kindred

Security Newsletter

8 Mar 2022

Subscribe to this newsletter

Critical Bugs Expose Hundreds of Thousands of Medical Devices and ATMs

Specialized health care devices, from imaging tools like CT scanners to diagnostic lab equipment, are often inadequately protected on hospital networks. Now, new findings about seven vulnerabilities in an Internet of Things remote management tool underscore the interconnected exposures in medical devices and the broader IoT ecosystem.

Researchers from the health care security firm CyberMDX, which was acquired last month by the IoT security firm Forescout, found seven easily exploited vulnerabilities, collectively dubbed Access:7, in the IoT remote access tool PTC Axeda.

The platform can be used with any embedded device, but has proven particularly popular in medical equipment. The researchers also found that some companies have used it to remotely manage ATMs, vending machines, barcode scanning systems, and some industrial manufacturing equipment.

Read More on Wired

More #News

- Dozens of COVID passport apps put user's privacy at risk
- Experts urge EU not to force insecure certificates in web browsers
- Social media phishing attacks are at an all time high
- Google Buys Cybersecurity Firm Mandiant for $5.4 Billion
- How to Automate Offboarding to Keep Your Company Safe
- U.S. Senate Passes Cybersecurity Bill to Strengthen Critical Infrastructure Security
- Strangest social engineering attacks of 2021

#Breach Log

- E-commerce giant Mercado Libre confirms source code data breach
- FBI: Ransomware gang breached 52 US critical infrastructure orgs
- Samsung confirms hackers stole Galaxy devices source code
- Malware now using stolen NVIDIA code signing certificates
- NVIDIA confirms data was stolen in recent cyberattack
- Axis Communications shares details on disruptive cyberattack

#Patch Time!

- CISA: Patch actively exploited Firefox zero-days until March 21st
- New Linux bug gives root on all major distros, exploit released
- Over 100,000 medical infusion pumps vulnerable to years old critical bug

#Tech and #Tools

- SharkBot: a “new” generation Android banking Trojan being distributed on Google Play Store
- Reports from the Field: Part 1
- The Dirty Pipe Vulnerability [CVE-2022-0847]
- Escaping privileged containers for fun
- New Linux Vulnerability CVE-2022-0492 Affecting Cgroups: Can Containers Escape?
- Samsung Encryption Flaw

This content was created by Kindred Group Security. Please share if you enjoyed!

Kindred Group in brief

Kindred Group is one of the world's leading online gambling operators with business across Europe, US and Australia, offering more than 30 million customers across 9 brands a great form of entertainment in a safe, fair and sustainable environment. The company, which employs about 2,000 people, is listed on Nasdaq Stockholm Large Cap and is a member of the European Gaming and Betting Association (EGBA) and founding member of IBIA (Sports Betting Integrity Association). Kindred Group is audited and certified by eCOGRA for compliance with the 2014 EU Recommendation on Consumer Protection and Responsible Gambling (2014/478/EU). Read more on www.kindredgroup.com.

You can access the previous newsletters at https://news.infosecgur.us