kindred

Security Newsletter

5 August 2019

Subscribe to this newsletter

'Urgent/11' Vulnerabilities Affect Many Embedded Systems

Security researchers with security vendor Armis have disclosed 11 different zero-day vulnerabilities within VxWorks, a real-time operating system used in some 2 billion embedded systems that include medical devices, routers, VOIP phones and even mission-critical infrastructure equipment, the company detailed on Monday. This collection of vulnerabilities, which Armis calls "Urgent//11," could lead to remote code execution and allow an attacker to take over a whole system without interacting with the user. Of the 11 flaws, six are deemed critical.

VxWorks is a widely-used real-time operating system that is owned and maintained by Wind River, headquartered in California. Unlike Microsoft Windows or Linux, these types of operating systems are found in various embedded and internet of things systems and typically process data quickly and allow for a high-degree of reliability. VxWorks has been deployed across different markets for more than 30 years and is still used in numerous embedded systems and IoT devices, including mission critical supervisory control and data acquisition systems, such as elevator and industrial controllers, as well as patient monitors, MRI machines, firewalls, routers, modems, VOIP phones and printers.

What also makes the vulnerabilities deemed critical a security concern is that the Armis researchers found that since flaws do not require user interaction, an exploit using remote code execution could spread malware from one vulnerable device to another within a network in the same way that the WannaCry ransomware and a newer Windows vulnerability called BlueKeep are both "wormable"

The URGENT/11 vulnerabilities affect all versions of the VxWorks software starting with the 6.5 release. The flaws, however, do not affect products designed for certification - such as VxWorks 653 and VxWorks Cert Edition - which are used by selected industries such as transportation, according to Armis.

Read More on bankinfosecurity

Even More on ARMIS blog

Capital One Data Breach Affects 106 Million People, Suspect Arrested

Capital One has announced a data breach that has exposed the personal information of 106 million people that includes transaction data, credit scores, payment history, balances, and for some, linked bank accounts and social security numbers. The data breach was discovered when a ethical hacker responsibly disclosed the vulnerability to Capital One on July 17th 2019. After performing an internal investigation of whether this vulnerability had been used in the past, Capital One discovered that an unauthorized used had access their systems and customer data between March 22nd and 23rd of 2019

Their investigation discovered that the unauthorized user was able to access the information for 100 million people in the United States and 6 million people in Canada. After fixing the vulnerability used in the breach, they provided information to the FBI who arrested the suspected hacker.

Due to the amount of personal information that was exposed and how it can be used for identity theft, it is strongly advised that users monitor their credit reports for suspicious activity and immediately report anything detected to both the police, Capital One, and the credit agencies. It is also strongly suggested that you freeze your credit report if you were affected to make it more difficult for bad actors to fraudulently take out credit in your name.

Read More on BleepingComputer

Even More on KrebsOnSecurity

More #News and #Breaches

- GDPR Enforcement Tracker
- Breach alert in South Korea after 1m card details were put up for sale online
- Researchers Replace IP Camera Feed With Fake Footage
- PCI Security Council, Retail ISAC Warn Retailers on Magecart Attacks
- Visa Contactless Cards Vulnerable to Fraudsters: Report
- Crooks Sell Credentials Using Combolists-as-a-Service Model
- REPORT: 82% of People Say They Connect to Any Free WiFi That's Available in a Public Place
- LAPD Data Breach Exposes Personal Info of Roughly 2.5K Officers
- Container Security Is Falling Behind Container Deployments
- Thinking more about bots and whether we do enough
- DMARC's abysmal adoption explains why email spoofing is still a thing
- Sephora Offers Monitoring Services in Wake of Data Breach
- Towards better vendor security assessments
- 3 strategies for building an information protection program

#Patch Time!

- Urgent11 security flaws impact routers, firewalls, printers, SCADA, and many IoT devices
- Google researchers disclose vulnerabilities for 'interactionless' iOS attacks
- Authenticated XSS Found in WordPress Plugin Facebook Widget

#Tech and #Tools

- Preventing The Capital One Breach
- PowerShell Empire Framework Is No Longer Maintained
- Identify Malicious Phishing Attacks with Outlook Conditional Formatting
- PhanTap: Red team network tap
- Cryptographic Attacks: A Guide for the Perplexed
- PowerHub: A post exploitation tool based on a web application
- Unveiling 11 New Adversary Playbooks
- Mapping your Blue Team to MITRE ATT&CK™
- Using Errant Callbacks to Enumerate and Evade Outlook's Sandbox
- 1.2GB of PowerShell in the wild
- Container Platform Security at Cruise
- Secrets Management in a Cloud Agnostic World
- Email Phishing Protection Guide – Enhancing Your Organization's Security Posture

Kingred Group is growing, so does the Group Security team! We're looking for new talented professionals to come join us:

- You like to break things, then explain how to fix it? Be part of our Cyber Security team
- You prefer the blue team side? Check out our Security analyst position
- Interested in Governance, Risk and Compliance? Apply for our Information Security Specialist role

Kindred is one of the largest online gambling companies in the world with over 24 million customers across 100 markets. You can find all our open vacancies on our career page.

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

Kindred Group in brief

Kindred is one of the largest online gambling companies in the world with over 24 million customers across 100 markets. We offer pre-game and live Sports betting, Poker, Casino and Games through 11 brands across our markets. We are committed to offer our customers the best deal and user experience possible, while ensuring a safe and fair gambling environment. Kindred is a pioneer in the online gambling industry and as an innovation driven company that builds on trust.

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