protiviti®
Face the Future with Confidence

It's Time to Take a Critical Look at the Security of Your IoT Devices . . . Now!

February 28, **2020**

Researchers at Singapore University of Technology and Design uncover major security vulnerabilities that could expose thousands of IoT devices to cyberattack

IoT Vulnerabilities on the Rise

A recently discovered set of Bluetooth-related vulnerabilities could mean thousands of IoT devices are vulnerable to attack and could experience deadlocks, crashes, buffer overflows and bypass of certain security settings. Researchers at the Singapore University of Technology and Design uncovered a set of 12 vulnerabilities affecting seven major system-on-a-chip (SoC) vendors whose chips are contained in more than 480 different IoT devices.[1] The review was not exhaustive, therefore potentially thousands of devices may be affected. Additionally, these SoC chipsets are some of the most popular in the world, so there is a high likelihood that many organizations have affected devices deployed in their environment and may be at risk. Protiviti has begun reviewing the vulnerabilities in our own security lab, and has validated that they are a serious, credible threat.

Potentially impacted devices include, but are not limited to:

- Medical devices
- Building automation
- Security systems
- Automotive devices
- Connected lighting devices
- Smart home products
- Consumer electronics

[1] Web site, "Unleashing Mayhem over Bluetooth Low Energy," February 11, 2020: https://asset-group.github.io/disclosures/sweyntooth/.

The researchers also published proof-of-concept exploit code, meaning they have demonstrated how the vulnerabilities can be exploited, and have made the code freely available to the public. This greatly increases the probability that cyber criminals will attempt to abuse these vulnerabilities in the near future. Organizations should immediately take action to determine if they have affected devices deployed in their environment and, if so, take steps to patch them or mitigate the risk of exploit.

The vulnerabilities affect the Bluetooth Low Energy (BLE) implementation within SoC chipsets. Bluetooth Low Energy is a wireless communication method that allows IoT and user devices such as a smartphone or iPad to communicate when the devices are within radio range (typically 10 to 20 meters). The identified vulnerabilities have different impacts ranging from crashing the device or causing it to lock and require a restart, to security control bypasses which can allow the attacker to write or read potentially sensitive data to or from the device, impact the confidentiality and integrity of transmitted data, and potentially modify or change settings and functions on the device. While all of these attack types could have major impact depending on the type or function of the device and processes it performs, the security bypass attack can have dramatic affects, some of which could have a serious impact on health, safety and security.

What should organizations do?

Companies that use or manufacture Bluetooth-enabled IoT devices should review the research for additional information, including specific details identifying the affected SoC chipsets, and take immediate action. Recommended measures include:

- Review IoT device inventory and determine if any of the devices use the affected chips.
- Contact the device vendors to determine if devices are affected by the vulnerabilities.
- For devices that have BLE capabilities, rank/prioritize devices in terms of need and potential impact to the business and determine if their BLE functionality can be disabled.
- If BLE cannot be disabled, ask the device vendor if a patch has been released or will be released, as well as the anticipated timeframe and how to apply the patch.
- For affected systems that cannot be patched, develop compensating controls such as restricting physical access to the devices to prevent an attacker from getting within BLE range.

- Monitor these devices for anomalous activity and educate users to be aware of the associated risks and attack methods.

While the research revealed an immediate need to review and manage the security of IoT devices employing specific SoC chipsets, it points to an even bigger need for a sound security strategy in this area. As the use of IoT becomes more pervasive and organizations employ more of these devices in their environments and businesses, it is important to remember that the security of these devices is not yet well understood. These devices carry unique risks that need to be managed, including a risk to confidential data. Organizations should develop an IoT strategy for managing, maintaining, securing and retiring IoT devices in their environments. The plan should include full lifecycle management of the devices from procurement through retirement, and should cover key controls such as asset management, security configuration, updates, secure communications, monitoring, resiliency and retirement. IoT devices should also be included in the organization's risk assessment so appropriate resources can be applied to manage the business risk this emerging technology presents to the organization.

How can Protiviti help?

Companies manufacturing or using IoT technology should consider several key questions:

- Does your company have an inventory of current assets with IoT capabilities being used within the organization?
- Do you have the capability to identify potential threats or monitor suspicious traffic on these devices?
- Do you have a plan and the skills and ability to update IoT devices if a security vulnerability is identified?
- Do you have controls in place to manage security and risks that IoT introduces to an organization?
- Do you have a technology and business resiliency plan?

Protiviti is uniquely positioned to help companies understand and manage the technical and business risks IoT technology carries. Our teams can help organizations develop and implement plans to manage the risks these devices bring, including standard development, device testing, IoT asset lifecycle management, monitoring, device management and resiliency planning.

About Protiviti

Protiviti is a global consulting firm that delivers deep expertise, objective insights, a tailored approach and unparalleled collaboration to help leaders confidently face the future. Through its network of more than 85 offices in over 25 countries, Protiviti and its independent and locally owned Member Firms provide clients with consulting solutions in finance, technology, operations, data, analytics, governance, risk and internal audit.

Named to the 2020 Fortune 100 Best Companies to Work For® list, Protiviti has served more than 60% of *Fortune* 1000® and 35% of *Fortune* Global 500® companies. The firm also works with smaller, growing companies, including those looking to go public, as well as with government agencies. Protiviti is a wholly owned subsidiary of Robert Half (NYSE: RHI). Founded in 1948, Robert Half is a member of the S&P 500 index.

Contact

Scott Laliberte
Global Leader Emerging Technologies Solutions
+1 267-256-8825
scott.laliberte@protiviti.com

© 2020 Protiviti Inc. An Equal Opportunity Employer M/F/Disability/Veterans.
Protiviti is not licensed or registered as a public accounting firm and does not issue opinions on financial statements or offer attestation services.

protiviti®