Karamba Security Blocks BlueBorne Bluetooth Flaws in Vehicle Electronic Control Units

Vehicle ECUs that run Linux and Android and are secured by Karamba's Autonomous Security are not exposed to newly discovered Bluetooth threats

ANN ARBOR, Mich. and HOD HASHARON, Israel — Sept. 14, 2017 – Devices protected by Karamba's Autonomous Security are not vulnerable to BlueBorne Bluetooth Flaws that can allow attackers to take over connected and autonomous vehicles.

What makes the BlueBorne flaws, revealed by security research firm Armis Security, so dangerous is that they use Bluetooth to insert malicious code in a target system. Even air-gapped devices or networks that aren't connected to the internet are vulnerable, since Bluetooth is a proximity communications method that doesn't need a wired connection. Bluetooth-equipped devices, such as Linux or Android in-vehicle infotainments, do not need to be in discoverable mode, or paired with the attacker's device to be vulnerable.

An in-depth analysis of the reports by security analysts at Karamba revealed that the attacks exploit vulnerabilities in the way the Bluetooth communication stack in Linux and Android devices manages memory, using a technique commonly referred to as buffer overflow. The attack allows full remote code execution on any Linux and Android device in Bluetooth range, and doesn't require any pairing or user interaction.

Another interesting point is that the attack researchers were able to bypass a common defense method, memory address space layout randomization (ASLR), by exploiting the inherent weaknesses of the ASLR technology and by exploiting other information leak vulnerabilities.

As explained by the Karamba Security researchers, the best protection against buffer overflow type vulnerabilities is to harden the code in the components used in devices according to their factory settings, thus preventing the execution of any foreign code, which is the malware.

Karamba's Autonomous Security would completely prevent attacks, such as the BlueBorne Bluetooth flaws, and any other threat whether known or unknown, by blocking the execution of foreign, malicious code at the component level.

Karamba Security, a provider of cybersecurity solutions for connected and autonomous vehicles, says this is just another example of why hardening sensors and electronic components is the only strategy that's going to prevent an attack.

"Security has to be designed in. We can't continually chase the next vulnerability with software patching," said Assaf Harel, Karamba Security CTO and co-founder. "It's ineffective in network computing and certainly won't work in vehicles, where Linux and Android operating systems are built in."

Harel also serves the industry by helping to develop, guide and influence cybersecurity best practices on the Automotive Grade Linux (AGL) Project under the auspices of The Linux Foundation.

Since coming out of stealth at the end of March 2016, Karamba Security has been actively engaged with 16 different ECU-hardening projects throughout the industry with car manufacturers and Tier-1 providers. In addition, Karamba was unanimously recognized with TU-Automotive's Best Cybersecurity Product/Service and the 2017 North American Frost & Sullivan Award for Automotive New Product Innovation.

More information is available at www.karambasecurity.com.

Resources
Autonomous Security
Karamba Security Approach
Karamba Security FAQ

About Karamba Security
Karamba Security provides industry-leading autonomous cybersecurity solutions for connected and autonomous vehicles. Karamba's software products automatically harden the ECUs of connected and autonomous cars, preventing hackers from manipulating and compromising those ECUs and hacking into the car. Karamba's Autonomous Security prevents cyberattacks with zero false positives, no connectivity requirements and negligible performance impact. In one year, Karamba has received a total investment of $17 million. The company has been recognized in 2017 with TU-Automotive's Best Cybersecurity Product/Service and the North American Frost & Sullivan Award for Automotive New Product Innovation. More information is available at www.karambasecurity.com.