Kudelski IoT Validates Microchip's CE1736 Trust Shield Controller for Use in Critical Data Center and Connected Systems

Hardware attack tests by Kudelski IoT's Advanced Security Lab ensure Microchip customers are getting a highly secure and robust real-time platform

Cheseaux-sur-Lausanne, Switzerland and Phoenix (AZ), USA – May 18, 2022 – Kudelski IoT, a division of the Kudelski Group (SIX: KUD.S), the world leader in digital security and IoT solutions, today announced that Microchip Technology has undergone advanced security testing of its CE1736 Trust Shield family of real-time platform root of trust microcontrollers. Done independently but in cooperation with Microchip, Kudelski IoT's Advanced Security Lab put the CE1736 family through multiple types of security attacks including advanced hardware attacks in an attempt to uncover vulnerabilities in the design and architecture that hackers could potentially use to compromise solutions, applications, and systems utilizing the part. The product was confirmed to reach the target security level set by Microchip.

The Microchip CEC1736 family is used in critical infrastructure for datacenters, telecommunication, networking systems, industrial and embedded computing settings where any vulnerability in security could cause irreparable harm to consumers, corporate enterprise and potentially national security. Real-time platform root of trust is used in applications and solutions when a device or server needs a strong security foundation, run-time firmware protection and an advanced cryptography for encryption/decryption. Securing systems against unauthorized firmware access goes beyond establishing a strong security foundation at boot. It also requires real-time firmware access monitoring, device attestation, and properly protecting a system throughout its entire lifecycle.

Kudelski IoT helps semiconductor and connected product companies evaluate the security of their existing products and helps them architect, define, and design future products with the right level of security for their target market. With a dramatic increase in high profile hacking cases such as the recent Colonial Pipeline attack, companies need to architect new products to withstand attacks that will occur over the product lifecycle.

"Security is not limited to a specification check-box item, it needs to be carefully designed from the start of a project, thoughtfully and effectively implemented, and then independently tested," said Joël Conus, Vice President of R&D at Kudelski IoT. "By working with us to validate the security of their CEC1736 Trust Shield family of parts, Microchip has shown their commitment to deliver a product to their customers that is robust against any threat it is likely to encounter in the field."

"Microchip has been working with Kudelski IoT for security device assessment and security architecture consulting across multiple device families. The Kudelski IoT team has unique expertise and conducts the most advanced attacks from the perspective of a hacker in a highly secure and trusted environment," said Ian Harris, vice president of Microchip's Computing Product Group. "It is essential to have an outside assessment of our products to ensure we avoid our own engineering biases and deliver the most secure possible product to our customers, and Kudelski IoT helps us achieve that."

About Kudelski IOT

Kudelski IoT is the Internet of Things division of Kudelski Group and provides end-to-end IoT solutions, IoT product design, and full-lifecycle services to IoT device manufacturers, ecosystem creators and end-user companies. These solutions and services leverage the group's 30+ years of innovation in digital business model creation; hardware, software and ecosystem design and testing; state-of-the-art security lifecycle management technologies and services and managed operation of complex systems. For more information about Kudelski IOT, please visit www.kudelski-iot.com.

About Kudelski Group

The Kudelski Group (SIX: KUD.S) is a world leader in digital business enablement technologies that encompass digital content security, public access, cybersecurity, and IoT.

NAGRA provides end-to-end convergent media solutions to the digital entertainment industry including services and applications requiring access control and rights management to secure the revenue in digital television, internet, mobile and interactive applications.

SKIDATA is the world market leader in public access and visitor management with over 10,000 installations in over 100 countries, providing fast and safe access for people and vehicles.

Kudelski Security is an innovative, independent provider of tailored cybersecurity solutions to help enterprises and public sector institutions assess risks and vulnerabilities and protect their data and systems.

Kudelski IoT provides end-to-end solutions, IoT product design, and full-lifecycle services to IoT device manufacturers, ecosystem creators and end-user companies.

The Kudelski Group is headquartered in Cheseaux-sur-Lausanne, Switzerland and Phoenix (AZ), USA with offices in 32 countries around the world. For more information, please visit www.nagra.com.

Media contacts

Christopher Schouten
Kudelski IoT
Marketing Director
+1 (480) 819-5781
christopher.schouten@nagra.com

Cédric Alber
Kudelski Group – Corporate Communications
Director Corporate Communications & Media Relations
+41 79 647 61 71
+1 (415) 962-5005
cedric.alber@nagra.com