Press Release 2020-620

**Cybersecurity:**

# Ripple20: LANCOM R&S®Unified Firewalls offer protection for millions of IoT devices

**Aachen, June 24, 2020—The world of the Internet of Things (IoT) is quaking. The reason is a set of critical security vulnerabilities collectively known as Ripple20. A vulnerable TCP/IP implementation is endangering millions of smart devices in private households, industrial plants and hospitals—and thus even human lives. Ripple20 has been rated by the US-CERT with the highest CVSS criticality score of 10 out of 10. Protection against these highly critical attacks is available with all LANCOM R&S®Unified Firewalls with full UTM functionality.**

Ripple20 targets the TCP/IP stack in hundreds of millions of IoT devices in all industries and sectors and makes them vulnerable to remote attacks. This includes networked power sockets, industrial control sensors, medical systems, and devices operating in critical infrastructures. The consequences can be dramatic: Incorrect sensor data can cause damage to industrial plant costing millions, and the general power supply could be massively disrupted. The hacking of infusion pumps or x-ray equipment in hospitals could endanger human lives. In office buildings or smart homes, doors can be opened or alarm systems deactivated without authorization.

Ripple20 was discovered by the security researchers at JSOF, who confirm the serious nature of the vulnerabilities: “An attacker can gain complete control over the targeted device remotely, with no user interaction required.” Just how critical these vulnerabilities are is also shown by the evaluation of the US-CERT with the highest score of 10 (out of 10) on the CVSSv3 scale.

**TCP/IP stack as a target for years to come – UTM firewalls offer protection**

Even though these security loopholes are not an issue for the current version of the TCP/IP stack, the problem remains because the majority of IoT devices and smart home devices simply cannot be updated. The vulnerable stack is likely to live on for years to come.

This is where LANCOM R&S® Firewalls provide the necessary protection. They detect and block the Ripple20 attack packets. The requirements are full UTM support, which is available in all models from the UF-200 upwards, and the activation of IPS/IDS. Signatures are updated daily to detect and block the malicious Ripple20 data packets.

When operated facing the Internet, a LANCOM R&S® Firewall shields the entire internal network behind it from dangerous attacks, including any IoT equipment and smart devices.

**LANCOM Systems background:**

LANCOM Systems GmbH is a leading European manufacturer of network and security solutions for business and the public sector. The portfolio includes hardware (WAN, LAN, WLAN, firewalls), virtual network components, and cloud-based software-defined networking (SDN).

Software and hardware development as well as manufacturing take place mainly in Germany, as does the hosting of the network management. There is a strong focus on trustworthiness and security. The company is committed to products that are free from backdoors and is a holder of the trust mark “IT Security Made in Germany” as initiated by the German Ministry of Economics.

LANCOM Systems was founded in 2002 and has its headquarters in Würselen near Aachen, Germany. Customers include SMEs, government agencies, institutions, and major corporations from all over the world. Since summer 2018, the company has been an independent subsidiary of the Munich-based technology group Rohde & Schwarz.

Your editorial staff contact:
Eckhart Traber
LANCOM Systems GmbH

Phone: +49 (0)89 665 61 78 - 67
Fax: +49 (0)89 665 61 78 - 97
press@lancom.eu
www.lancom.eu

Sabine Haimerl
vibrio Kommunikationsmanagement Dr. Kausch GmbH
Phone: +49 (0)89 32151 - 869
Fax: +49 (0)89 32151 - 70
lancom@vibrio.de
www.vibrio.eu