Ripple20: LANCOM Unified Firewalls bieten Schutz für Millionen von IoT-Devices

24.06.2020

.

Pressemitteilung 2020-620

Download PDF

Cybersecurity:

Ripple20: R&S®LANCOM Unified Firewalls bieten Schutz für Millionen von IoT-Devices

Aachen, 24. Juni 2020 – Die Welt der Internet of Things (IoT) bebt. Grund dafür ist eine Reihe kritischer Sicherheitslücken, die unter dem Namen Ripple20 bekannt wurden. Die anfällige TCP/IP-Implementierung gefährdet Abermillionen smarter Geräte in privaten Haushalten, Industrieanlagen und Krankenhäusern und damit sogar Menschenleben. Ripple20 wurde vom US-CERT mit der höchsten CVSS-Kritikalitätsstufe (10 von 10) bewertet. Schutz vor den hochkritischen Angriffen bieten alle R&S®LANCOM Unified Firewalls mit vollständiger UTM-Funktionalität.

Ripple20 betrifft den TCP/IP-Stack von Hunderten Millionen IoT-Geräten in allen Branchen und Bereichen und macht sie anfällig für Remote-Angriffe. Darunter vernetzte Steckdosen, aber auch industrielle Steuerungssensoren und medizinische Systeme und Geräte, die in kritischen Infrastrukturen eingesetzt werden. Mit teils dramatischen Folgen: Falsche Sensordaten können in Industrieanlagen Millionenschäden verursachen, die Stromversorgung massiv gestört werden. Gehackte Infusionspumpen oder Röntgengeräte in Krankenhäusern gefährden Menschenleben. In Bürogebäuden oder Smart-Homes lassen sich unbefugt Türen öffnen oder Alarmanlagen deaktivieren.

Die Entdecker von Ripple20, die Sicherheitsforscher des Unternehmens JSOF bestätigen die Schwere der Lücken: „Ein Angreifer kann die vollständige Kontrolle über das Zielgerät aus der Ferne erlangen, ohne dass eine Benutzerinteraktion erforderlich ist.“ Wie kritisch die gefundenen Lücken sind, zeigt auch die Bewertung des US-CERT mit der höchsten Stufe 10 (von 10) auf der CVSSv3-Skala.

TCP/IP-Stack noch Jahre als Angriffsziel – UTM-Firewalls schützen

Zwar sind die Sicherheitslücken in der aktuellsten Version des TCP/IP-Stacks geschlossen. Das Problem bleibt aber bestehen, da der Großteil der IoT-Devices und Smart Home-Geräte sich schlicht nicht aktualisieren lässt und der verwundbare Stack damit noch viele Jahre weiterleben dürfte.

Für solche Fälle bieten die LANCOM R&S® Firewalls den nötigen Schutz. Sie können die Angriffspakete von Ripple20 erkennen und blockieren. Voraussetzung ist die vollständige UTM-Unterstützung, die in allen Modellen ab der UF-200 aufwärts vorhanden ist, und die Aktivierung von IPS/IDS. Dessen Signaturen werden täglich aktualisiert, wodurch bösartige Ripple20-Datenpakete erkannt und blockiert werden.

An der Grenze zum Internet eingesetzt, schützen die LANCOM R&S® Firewalls das gesamte dahinterliegende interne Netzwerk mit allen IoT-Devices und smarten Geräten vor den gefährlichen Angriffen.

Hintergrund LANCOM Systems:

Die Rohde & Schwarz Networks and Cybersecurity GmbH ist führender europäischer Hersteller von Netzwerk- und Security-Lösungen für Wirtschaft und Verwaltung. Das Portfolio umfasst Hardware (WAN, LAN, WLAN, Firewalls), virtuelle Netzwerkkomponenten und Cloud-

basierendes Software-defined Networking (SDN).

Soft- und Hardware-Entwicklung sowie Fertigung finden hauptsächlich in Deutschland statt, ebenso wie das Hosting des Netzwerk-Managements. Besonderes Augenmerk gilt der Vertrauenswürdigkeit und Sicherheit. Das Unternehmen hat sich der Backdoor-Freiheit seiner Produkte verpflichtet und ist Träger des vom Bundeswirtschaftsministerium initiierten Vertrauenszeichens „IT-Security Made in Germany".

LANCOM wurde 2002 gegründet und hat seinen Hauptsitz in Würselen bei Aachen. Zu den Kunden zählen KMU, Behörden, Institutionen und Großkonzerne aus aller Welt. Seit Sommer 2018 ist das Unternehmen eigenständige Tochtergesellschaft des Münchner Technologiekonzerns Rohde & Schwarz.

Ihr Redaktionskontakt:

Eckhart Traber

Rohde & Schwarz Networks and Cybersecurity GmbH

Tel: +49 (0)89 665 61 78 - 67

Fax: +49 (0)89 665 61 78 - 97

presse@lancom.de

www.lancom.de

Sabine Haimerl

vibrio Kommunikationsmanagement Dr. Kausch GmbH

Tel: +49 (0)89 32151 - 869

Fax: +49 (0)89 32151 - 70

lancom@vibrio.de

www.vibrio.eu