Legnago, 24 March 2022

# *Critical vulnerability TLStorm*

**Subject: CVE-2022-22805 – (CVSS 9.0) TLS buffer overflow, CVE-2022-22806 – (CVSS 9.0) TLS authentication bypass, CVE-2022-0715 – (CVSS 8.9) Unsigned firmware upgrade that can be updated over the network (RCE).**

**CVE-2022-22805 – (CVSS 9.0) TLS buffer overflow: A memory corruption bug in packet reassembly (RCE).**

**CVE-2022-22806 – (CVSS 9.0) TLS authentication bypass: A state confusion in the TLS handshake leads to authentication bypass, leading to remote code execution (RCE) using a network firmware upgrade.**

**CVE-2022-0715 – (CVSS 8.9) Unsigned firmware upgrade that can be updated over the network (RCE).**

The firmware version **2.xx and 3.xx**, available for Netman 204 are not affected by CVE-2022-22805, CVE-2022-22806 and CVE-2022-0715.

Two of the vulnerabilities involve the TLS connection between the UPS from another brand and its cloud service. Devices that support the cloud connection feature automatically establish a TLS connection upon startup or whenever cloud connections are temporarily lost. Attackers can trigger the vulnerabilities via unauthenticated network packets without any user interaction

The third vulnerability is a design flaw in which the firmware updates on affected devices are not cryptographically signed in a secure manner. As a result, an attacker could craft malicious firmware and install it using various paths, including the Internet, LAN, or a USB thumb drive. This modified firmware could allow attackers to establish long-lasting persistence on such UPS devices that can be used as a stronghold within the network to launch additional attacks.

Riello UPS ensure his customers that **no one of the listed vulnerabilities affect Netman 204 network card and any its UPS as well**.

Massimo Zampieri

*Single Phase PM*

RPS S.p.A.