

June 28, 2024

Legrand -ServerTech, engaged CBIZ Pivot Point Security (CPPS) to conduct an IoT security assessment, and penetration test utilizing our CREST accredited testing methodology against a ServerTech Pro4x PDU. The testing was performed in June of 2024 on hardware version A1, running firmware version 4.2.10-5-50400.

Our comprehensive IoT device security assessment methodology is derived from industry best practices, including the Open-Source Security Testing Methodology Manual (OSSTMM), the Penetration Testing Execution Standard (PTES), the OWASP Firmware Security Testing Methodology, and our 15+ years of technical testing experience. We scale this Council for Registered Ethical Security Testers (CREST) accredited methodology to account for differing risks and business objectives to optimize the assurance provided by our testing. Our testing included:

- Full testing of the device's exposed services from a network perspective.
- An OWASP Top 10 assessment of any exposed applications on the device.
- A full assessment of communication channels security.
- An assessment of the physical security of the device.
- A hardware security assessment of the device's 'internals'.
- Binary and reverse engineering analysis of the device's firmware.

We determined that the ServerTech Pro4x PDU was secured in a manner consistent with industry best practices, CA SB 327, NISTIR 8259, and on par with peer devices that we have tested.

CBIZ Pivot Point Security has been architected to provide maximum levels of independent and objective information security expertise to our varied client base. The team responsible for conducting security assessments of this nature is led by a Certified Information Security Auditor/IRCA ISO 27001 Auditor and includes personnel appropriately qualified to render this opinion (e.g., Certified Information System Security Professionals, Offensive Security Certified Professionals, etc.).

If you have any questions regarding this attestation, please contact me at 1-888-748-6876.



John Verry, 27001-CLA/CISA/CRISC/CTPRP

Principal Enterprise Security Consultant

