Security Response 09122024-001

The Cybersecurity Assessment Requirements for RED Article 3.3
As they pertain to Multi-Tech Products

Initial Publication Date: September 12, 2024

Overview
While we may not have test or assessment methods and procedures yet, we do now know the content of the standardization request and therefore we do know what the requirements are that equipment will need to meet, from 1 August 2025 onwards.

For all of the RED Article 3.3 parts, it is assumed that the first versions of the cybersecurity standards will set assessment levels for the fundamental requirements, to get all radio equipment within scope of the requirement up to a reasonable level of security. Some equipment likely has no existing cybersecurity or resilience, and the first stage will be to bring all equipment to a suitable minimum level of acceptable security.

We know the following about the three applicable aspects of RED Article 3.3:

Article 3.3(d)
<u>Summary</u>

- Radio equipment does not harm the network or its functioning nor misuse network resources, thereby causing an unacceptable degradation of service
- **MultiTech products currently support Article 3.3(d)**

<u>Overview</u>
This clause is applicable to equipment that connects to the internet, directly or indirectly.

The radio equipment shall:

(a) Include elements to monitor and control network traffic, including the transmission of outgoing data
(b) Be designed to mitigate the effects of ongoing denial of service attacks
(c) (Implement appropriate authentication and access control mechanisms
(d) Be provided, on a risk basis, with up-to-date software and hardware at the moment of placing on the market that do not contain publicly known exploitable vulnerabilities as regards harm to the network or its functioning or misuse of network resources
(e) Be provided with automated and secure mechanisms for updating software or firmware that allow, when necessary, the mitigation of vulnerabilities that if exploited may lead to the radio equipment harming the network or its functioning or the misuse of network resources
(f) Protect the exposed attack surfaces and minimize the impact of successful attacks

Article 3.3(e)

Summary

- Radio equipment incorporates safeguards to ensure that the personal data and privacy of the user and the subscriber are protected
- **Article 3.3(e) does not apply to MultiTech products**

Overview

This clause is applicable to equipment that is capable of processing personal data, traffic data, or location data. Also, equipment exclusively for childcare, equipment that may worn on, strapped to, or hung from any part of the head or body, including clothing, and other internet-connected equipment.

The radio equipment shall:

(a) Protect stored, transmitted, or otherwise processed personal data against accidental or unauthorized processing, including storage, access, disclosure, destruction, loss or alteration or lack of availability
(b) Implement appropriate authentication and access control mechanisms
(c) Be provided, on a risk basis, with up-to-date software and hardware at the moment of placing on the market that does not contain publicly known exploitable vulnerabilities as regards data protection and privacy
(d) Be provided with automated and secure mechanisms for updating software or firmware that allow, when necessary, the mitigation of vulnerabilities that if exploited may lead to unauthorized processing, including storage, access, disclosure, destruction, loss or alteration, or lack of availability of personal data
(e) Include functionalities to inform the user of changes that may affect data protection and privacy
(f) Log the internal activity that can have an impact on data protection and privacy
(g) Allow users to easily delete their stored personal data, enabling the disposal or replacement of equipment without the risk of exposing personal data
(h) Protect the exposed attack surfaces and minimize the impact of successful attacks

The standardization request clarifies that it is important for assessments of smartphones, equipment for childcare, radio-enabled toys, smart meters, and 5G networks shall consider other regulations and not undermine the assessments covered by such regulations.

Article 3.3(f)

Summary

- Radio equipment supports certain features ensuring protection from fraud
- **Article 3.3(f) does not apply to MultiTech products**

Overview

This clause is applicable to equipment that connects to the internet, directly or indirectly and allows the user to transfer money, monetary value, or virtual currency.

The radio equipment shall:

(a) Protect stored, transmitted, or otherwise processed financial or monetary data against accidental or unauthorized processing, including storage, access, disclosure, destruction, loss or alteration or lack of availability

(b) Implement appropriate authentication and access control mechanisms

(c) Be provided, on a risk basis, with up-to-date software and hardware at the moment of placing on the market that does not contain publicly known exploitable vulnerabilities as regards financial or monetary data

(d) Be provided with automated and secure mechanisms for updating software or firmware that allow, when necessary, the mitigation of vulnerabilities that if exploited may lead to unauthorized processing, including storage, access, disclosure, destruction, loss or alteration, or lack of availability of financial or monetary data

(e) Log the internal activity that can have an impact on financial or monetary data

(f) Protect the exposed attack surfaces and minimize the impact of successful attacks

MultiTech Product Impacted in This Response

Conduit® 300

The Conduit® 300 Series programmable gateway featuring mPower™ Edge Intelligence enables streamlined edge-to-cloud orchestration, management and analytics together with a high performance, secure processor to support Dockers and containers for easy programmability and built-in compatibility with leading IoT software platforms. mPower Edge Intelligence incorporates a host of security features including signed firmware validation, enhanced firewall and VPN settings, secure authentication and more.

Conduit® AP

The Conduit AP conveniently provides deep in-building connectivity and improved performance for network operators and enterprises connecting thousands of IoT assets by harnessing the power of the LoRaWAN® protocol.

Conduit® IP67 and Conduit® IP67 200

The Conduit® IP67 200 Series Base Station is a ruggedized IoT gateway solution, specifically designed for outdoor LoRa® public or private network deployments. This highly scalable and certified IP67 solution can resist the harshest environmental factors including moisture, dust, wind, rain, snow and extreme heat, supporting LoRaWAN® applications in virtually any environment.

Conduit®

The Conduit® gateway is the industry's most configurable, manageable, and scalable LoRa® gateway for industrial IoT applications. Network connectivity choices to your preferred data management platform include carrier approved 4G-LTE, 3G and Ethernet.

rCell 300

The rCell 300 Series industrial cellular routers are optimized for secure M2M (machine-to-machine)/Internet of Things (IoT) applications, with mPower™ Edge Intelligence embedded software, offering a robust Ethernet or serial network interface platform ready to deploy.

MultiConnect® rCell 100 Series

The MultiConnect® rCell 100 series of industrial cellular routers, optimized for secure M2M (machine-to-machine) and Internet of Things (IoT) applications, offer a Ethernet or serial network interface platform ready to deploy.

Overview of MultiTech Approach to Cybersecurity

MultiTech uses the National Institute of Standards and Technology (NIST) Cybersecurity Framework, which provides a comprehensive approach to cybersecurity that addresses cybersecurity, not only at an organizational level, but also with specific frameworks for manufacturers of IoT devices.

As the designer and manufacturer of IoT devices, MultiTech security begins with the organization itself and the Company has completed a thorough evaluation of its systems and processes against the NIST CSF to ensure the ongoing integrity of its operations. As a result of its adherence to security standards, all IoT devices manufactured at MultiTech implement core capabilities, as defined by NIST Interagency Reports (NISTIR) for IoT devices.

MultiTech Corporate Highlights

- 3rd party, 24/7 **MDR (Managed Detection and Response)** vulnerability monitoring
- Ongoing vulnerability scans of systems, websites, and services
- Cybersecurity insurance requiring **2-factor authentication** for access
- **SAT** (Security Awareness Training) for all employees Compliance Standards
- **SoC 2** (System and Organization Controls) – Protecting customer data
- **ISO 27001** – Information Security Compliance (roadmap) Manufacturing
- **Air-gapped** manufacturing networks are isolated from other enterprise systems and the Internet

Cybersecurity Incident Response Team (CSIRT)

- A dedicated team to respond to changing security threats in the market, including active monitoring of threats (e.g. CVEs) and taking related actions
- International Security Agencies
  - NIST – National Institute of Standards and Technology
  - The MITRE Corporation (https://www.cve.org)
- Regional Security Standards
  - Cyber Resilience Act – EU
  - PTSI – UK
  - California AB 1906 – US
  - ANATEL ACT 77 – Brazil

Cybersecurity Incident Response Process (CSIRP)

1. Discovery
   - Periodic penetration (PEN) testing performed by MultiTech, third parties and customers
   - Public announcements
2. Triage
   - Understand the severity and impact on MultiTech devices, operating systems, and services
   - Set an action plan
3. Advisory
   - Publish a security advisory disclosing the products impacted and the products not impacted
   - www.multitech.com/landing-pages/security
4. Remediation
   - Provide software updates for customers
   - Communicate availability in product change notifications (PCNs) and software release notes

Additional Information

If you have any questions regarding this Security Response, please contact your MultiTech sales representative or visit the technical resources listed below:

World Headquarters – USA
+1 (763) 785-3500 | sales@multitech.com

EMEA – UK
+(44) 118 959 7774 | sales@multitech.co.uk

MultiTech Security Advisories
www.multitech.com/landing-pages/security
MultiTech monitors industry news and announcements to identify security issues that may impact our devices and operating systems and strives to provide the information and tools to keep your deployments secure and online.

MultiTech Developer Resources
www.multitech.net
An open environment where you can ask development related questions and hear back from MultiTech engineering or a member of this community.

MultiTech Support Portal
support.multitech.com
Create an account and submit a support case directly to our technical support team.

MultiTech Website
www.multitech.com

Trademarks and Registered Trademarks
Conduit, MultiConnect, MultiTech and the MultiTech logo are registered trademarks of Multi-Tech Systems, Inc. All other trademarks or registered trademarks are the property of their respective owners.

Revision History

Version	Author	Date	Change Description
DT,	DT, DW, TG	09/12/2024	Initial Publication