# Cybersecurity of MultiTech IoT Gateways and Routers

IoT systems and devices have become an integral part of organizations infrastructure and business processes. Enablers behind digital transformation programs, these new technologies improve costs, efficiency, compliance and sustainability. They also, however present a significant security challenge for IT departments, as their scope is vast and often unique compared to conventional IT devices.

MultiTech recognizes that Cybersecurity is critical to IoT systems.  As a leading manufacturer of IoT devices used in business critical, commercial, and industrial applications MultiTech works continuously to ensure its devices are both secure and securable within larger integrated systems.

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.

A remaining challenge for organizations implementing IoT systems involves understanding the differences between conventional IT devices and IoT devices. A June 2019, study, published by NISTIR 8228, specifically identifies the expectations of conventional IT devices and the challenges IoT devices might pose to those expectations. The paper discusses how MultiTech IoT Gateways and Routers address those expectations and provides guidance for IT and engineering teams to ensure the security and securability of their IoT systems.

## NISTIR 8228 Challenges for Individual IoT Devices and MultiTech Response

| Asset Management | MultiTech IoT Gateways and Routers |
|---|---|
| Expectation 1: The device has a built-in unique identifier. | Devices identify using credentials managed in TPM2.0 (e.g., Conduit300) or in open memory (other devices). Credentials are provisioned either manually by user or at device birth. |
| Expectation 2: The device can interface with enterprise asset management systems. | Devices offer DeviceHQ management client interfacing with public or private cloud-based DeviceHQ device management service. Devices identify using credentials managed in TPM2.0 (e.g., Conduit300) or in open memory (other devices). Credentials are provisioned either manually by user or at device birth. |
| Expectation 3: The device can provide the organization sufficient visibility into its characteristics | Devices offer both visibility and configurability of devices' hardware and software through DeviceHQ. |
| Expectation 4: The device or the device's manufacturer can inform the organization of all external software and services the device uses, such as software running on or dynamically downloaded from the cloud. | Devices' dependencies on external software and services are well documented such as firmware updates, DeviceHQ service, and LoRa network server service. |
| **Vulnerability Management** | |
| Expectation 5: The manufacturer will provide patches or upgrades for all software and firmware throughout each device's lifespan. | Firmware update and patch release policies are well documented and outline the related timeframes and methods. |
| | Firmware update and patch release policies are well documented and outline the related timeframes and methods. |
| Expectation 6: The device either has its own secure built-in patch, upgrade, and configuration management capabilities, or can interface with enterprise vulnerability management systems with such capabilities. | Firmware update and patch can be accomplished through DeviceHQ. Known firmware and patch behavior including potential problems is well documented in related documentation such that customers can prepare appropriate deployment and verification plans. Centralized vulnerability management systems may be compatible with MultiTech firmware APIs (application protocol interfaces), specific requirements should be discussed with MultiTech. |
| Expectation 7: The device either supports the use of vulnerability scanners or provides built-in vulnerability identification and reporting capabilities. | PEN testing, binary analysis and CVE (Common Vulnerabilities and Exposures) analysis can be performed. No internal mechanism for vulnerability reporting due to limited compute platform resources and requirement not to degrade user available device performance. |
| **Access Management** | |
| Expectation 8: The device can uniquely identify each user, device, and process attempting to logically access it. | Users accessing device, the device itself, and CPU platform processes are all uniquely identified, e g device-id, TPM on select devices, and unique self-signed certificates. |
| Expectation 9: The device can conceal password characters from display when a person enters a password for a device, such as on a keyboard or touch screen. | Concealment of password characters is supported. |
| Expectation 10: The device can authenticate each user, device, and process attempting to logically access it. | No default password; this must be set at first boot. Password complexity rules are supported. Multifactor authentication can be supported if required. RADIUS supported. |
| Expectation 11: The device can use existing enterprise authenticators and authentication mechanisms. | RADIUS supported. WiFi support can be implemented if required. |
| Expectation 12: The device can restrict each user, device, and process to the minimum logical access privileges necessary. | User personas' rights can be defined. TOMOYO is supported for processes. Custom user roles support under development. MAC Security supported. |
| Expectation 13: The device can thwart attempts to gain unauthorized access, and this feature can be configured or disabled to avoid undesired disruptions to availability. (Examples include locking or disabling an account when there are too many consecutive failed authentication attempts, delaying additional authentication attempts after failed attempts, and locking or terminating idle sessions.) | Repeat failed user access attempts result in disabling access. Thresholds and timeouts for login failure lockouts are configurable. |
| Expectation 14: The device has adequate built-in physical security controls to protect it from tampering (e.g., tamper-resistant packaging). | No physical security included. The solutions integrator should ensure that the installation is physically secure. |

## NISTIR 8228 Challenges for Individual IoT Devices and MultiTech Response

| Asset Management | MultiTech IoT Gateways and Routers |
|---|---|
| **Incident Detection** | |
| Expectation 15: The device can log its operational and security events. | Security relevant logging is done at appropriate syslog levels. No physical security included. The solutions integrator should ensure that the installation is physically secure. |
| Expectation 16: The device can interface with existing enterprise log management systems. | Syslog supported. Additional interfacing with an IDS or other security device is not supported. |
| Expectation 17: The device can facilitate the detection of potential incidents by internal or external controls, such as intrusion prevention systems, anti-malware utilities, and file integrity checking mechanisms. | Compute platform architecture dependent. Exportable logging supported. MAC control logging violations supported. |
| Expectation 18: The device can support event and incident analysis activities. | Compute platform architecture dependent. |
| Expectation 19: The device can prevent unauthorized access to all sensitive data on its storage devices. | Compute platform architecture dependent. User data encryption supported/can be supported, with or without root of trust |
| | Linux kernel options to sanitize user data before erasing on factory reset. Root file system is read-only. Factory reset erases overlay and leaves device with original read-only root file system. |
| Expectation 20: The device has a mechanism to support data availability through secure backups. | User configuration can be managed through DeviceHQ. Users can download configuration copy for backup. User defined defaults capability supports local configuration backup and restore |
| Expectation 21: The device can prevent unauthorized access to all sensitive data transmitted from it over networks. | LoRaWAN communication is inherently encrypted. Encryption over other communication channels to be managed in application domain. OpenSSL 1.1.1 provides sufficient encryption for any protocol using it. Defaults used are per industry best practices. User data encryption on CPU platform is robust and secure. |
| Expectation 22: The device operates in a traditional federated identity environment. | RADIUS authentication for non-local users supported. |
| **Informed Decision Making** | |
| PII (Personally Identifiable Information) Processing Permissions Management | |
| Expectation 24: There is sufficient centralized control to apply policy or regulatory requirements to PII. | No PII is collected by or stored in the device. |
| **Information Flow Management** | |
| Expectation 25: There is sufficient centralized control to manage PII. | No PII is collected by or stored in the device. |


World Headquarters

Multi-Tech Systems, Inc.
2205 Woodale Drive
Mounds View, MN 55112 U.S.A.
Tel: 763-785-3500
Email: sales@multitech.com
www.multitech.com


MULTITECH®

CONNECT WITH MULTITECH