MULTITECH WHITE PAPER

Cybersecurity, RED-DA & the Cyber Resilience Act

A compliance summary for distributors, integrators, and end customers

ABOUT THIS WHITE PAPER

As the European Union moves cybersecurity for connected products from voluntary best practice into enforceable law, MultiTech is helping its channel partners and end customers stay ahead of every deadline. This white paper sets out how MultiTech IoT gateways, routers, and modems meet the Radio Equipment Directive Delegated Act (RED-DA) — mandatory since August 1, 2025 — and how we are preparing for full Cyber Resilience Act (CRA) enforcement in December 2027. It is written for two audiences: distributors who need to keep compliant product flowing through their channels, and integrators who need to inherit our compliance work cleanly into their own deployments.

Document 86003004 · May 2026

Supersedes MultiTech RED-DA Compliance Summary 09122024-001 (September 2024).

Executive Summary

Two EU regulations now govern cybersecurity for the kind of connected products MultiTech makes. The Radio Equipment Directive Delegated Act (RED-DA, EN 18031) has been mandatory since August 1, 2025. The Cyber Resilience Act (CRA, Regulation (EU) 2024/2847) entered into force in December 2024, with vulnerability and incident reporting obligations applying from September 11, 2026 and full conformity, CE marking, and lifecycle obligations from December 11, 2027. Together, they raise the floor for what every internet-connected product placed on the EU market must do.

MultiTech has assessed its in-scope portfolio and confirmed RED-DA conformity against the harmonized EN 18031-1, -2, and -3 standards. CE marking, self-signed EU Declarations of Conformity, and technical documentation are available for each in-scope product family. CRA readiness is well underway: a Software Bill of Materials is maintained for mPower and the major hardware platforms, a Coordinated Vulnerability Disclosure process is in place at multitech.com/security/, and our Cybersecurity Incident Response Team is being aligned to the CRA's 24-hour/72-hour/14-day reporting clock ahead of the September 2026 deadline.

For distributors, the practical implication is straightforward: stock and resell only product with current CE marking and supporting documentation, forward MultiTech security advisories promptly, and route any customer-reported vulnerability or incident to our CSIRT within 24 hours. For integrators and end customers, MultiTech provides the device-level controls (secure-by-default configuration, signed firmware, TLS, TPM-backed identity, RADIUS, syslog export); responsibility for application-layer policy and physical site security remains with the deployment owner. Penalties under the CRA reach €15 million or 2.5% of global annual turnover for serious violations — compliance is no longer optional.

The remainder of this paper details how RED-DA and the CRA fit together, MultiTech's compliance status against each requirement, and concrete implementation guidance for both audiences. An appendix maps MultiTech platform capabilities to the U.S. NIST framework for IoT cybersecurity (NISTIR 8228) for integrators using that reference.

Contents

Why This Matters Now

The EU has moved cybersecurity for connected products from voluntary best practice to enforceable law. Two regulations apply to MultiTech-class products, and they overlap but do not replace each other:

- **RED-DA (EN 18031):** In force since August 1, 2025. Cybersecurity essential requirements under Article 3.3(d), (e), and (f) of the Radio Equipment Directive 2014/53/EU for any internet-connected radio equipment placed on the EU market.
- **Cyber Resilience Act (Regulation (EU) 2024/2847):** Entered into force December 2024. Vulnerability and incident reporting obligations apply from September 11, 2026. Full conformity, CE marking, and lifecycle obligations apply from December 11, 2027.

Penalties under the CRA are substantial — **up to €15 million or 2.5% of global annual turnover** for serious violations. Beyond fines, non-compliance means losing the right to sell in the EU. MultiTech is investing now so our distributors and customers do not have to scramble later.

RED-DA and the CRA: How They Fit Together

Both regulations push manufacturers toward the same outcomes — secure connections, protected data, prompt vulnerability response — but they apply differently. The table below sets out where they diverge so distributors and customers can plan.

Dimension	RED-DA (EN 18031)	Cyber Resilience Act (CRA)
Scope	Internet-connected radio equipment only.	All products with digital elements that connect directly or indirectly to a network.
In force	Mandatory since 1 August 2025.	In force December 2024. Reporting obligations: 11 September 2026. Full obligations: 11 December 2027.
Core requirements	Network protection, personal-data protection, fraud prevention (Art. 3.3 d/e/f).	Secure-by-design, vulnerability handling, SBOM, secure updates, incident reporting, conformity assessment.
Documentation	Technical file and self-signed EU Declaration of Conformity.	Technical documentation retained 10 years or for the support period (≥ 5 years), plus SBOM and risk assessment.
Conformity route	Self-assessment for harmonized-standards compliance, or Notified Body where applicable.	Self-assessment for default class; third-party assessment for Critical Class I/II products (Annex III/IV).
Reporting	Handled through existing market-surveillance channels.	Actively exploited vulnerabilities and severe incidents notified to ENISA and the coordinating CSIRT — early warning within 24 h, follow-up at 72 h, final report at 14 days.

Bottom line: RED-DA is the rule MultiTech products are being placed on the EU market under today. The CRA is what every connected product will be measured against from December 2027 onward. Our compliance work is designed to satisfy both.

RED-DA Status: Compliant

MultiTech has assessed its in-scope product portfolio — gateways, routers, and modems with wired or wireless internet connectivity — and confirmed RED-DA conformity against the harmonized standards EN 18031-1, EN 18031-2, and EN 18031-3.

How we map to Article 3.3

Article	Requirement	MultiTech Implementation
3.3(d)	Network protection — prevent unauthorized access and harm to the network	TLS with current OpenSSL (3.0.13 in mPower 7.4), certificate-based access, configurable firewall rules, RADIUS and WPA2-Enterprise (802.1X) authentication, no default password, minimum 15-character passwords on commissioned devices.
3.3(e)	Protection of personal data and privacy	Encryption for data in transit and at rest, read-only root filesystem, factory-reset sanitization of user data, secure storage of credentials in TPM 2.0 on AP300-class hardware. MultiTech devices do not collect or store PII themselves; integrators retain control of personal data flows.
3.3(f)	Protection against financial fraud	Not applicable — MultiTech products do not process financial transactions or act as payment interfaces. Documented in the technical file with justification.

What MultiTech provides today

- **EU Declaration of Conformity** (self-signed, harmonized-standards route) available for each in-scope product family.
- **Technical documentation** covering risk assessment, asset mapping to EN 18031, test evidence, and lifecycle controls — retained for the period required by RED-DA and aligned to the longer CRA retention rules.
- **CE marking** applied to all RED-DA-compliant units placed on the EU market on or after 1 August 2025.
- **Product Change Notifications (PCNs)** issued through our standard channels whenever a compliance-relevant firmware or hardware change is released.

Devices placed on the EU market before 1 August 2025 remain saleable under the prior regime. **New stock manufactured after that date, and any product receiving a significant update, is supplied as RED-DA compliant.**

CRA Readiness: What We're Doing Now

RED-DA is the foundation. The CRA extends those same principles across the full product lifecycle and adds new obligations — most notably formal vulnerability disclosure, SBOM management, and 24-hour reporting to ENISA. Here is where MultiTech stands against the CRA's core pillars.

Secure by design

Cybersecurity is built into the MultiTech development lifecycle, not bolted on. Every product line undergoes threat modeling, secure code review, third-party penetration testing, binary analysis, and

CVE triage before release. Devices ship without default passwords, with secure-by-default configurations, and with attack surface deliberately minimized — interfaces and services are off in the factory-default state unless they are essential.

Vulnerability handling and SBOM

- **SBOM.** MultiTech maintains a Software Bill of Materials for mPower and major hardware platforms. Continuous monitoring against the MITRE CVE database and upstream advisories drives our patch pipeline. Recent examples include the OpenSSH 9.8p1 upgrade addressing CVE-2024-6387.
- **Coordinated Vulnerability Disclosure (CVD).** A public security contact and intake process is published at multitech.com/security/. Reports are triaged by the MultiTech CSIRT under our documented Cybersecurity Incident Response Process.
- **Customer notification.** Security advisories are published publicly, and impacted customers receive PCNs and release notes describing the issue, severity, and remediation.

Secure updates throughout the support period

MultiTech firmware is delivered signed and authenticated, with rollback prevention and a documented update validation procedure. Updates can be deployed at scale through DeviceHQ — our cloud-based device management service available as a public or private deployment — or staged manually by integrators that prefer local control. Support periods and update commitments are published per product family and meet or exceed the CRA's five-year floor.

Conformity assessment and documentation

MultiTech's products fall within the CRA default class, supporting the internal-control conformity route. Where future product features cross into Critical Class I or II (Annex III), MultiTech will engage a Notified Body. Our technical file already includes the architecture documentation, risk assessment, test evidence, update mechanism description, and SBOM that the CRA requires under Annex II and Annex VII.

Reporting readiness

The CSIRT is structured to meet the CRA's reporting clock: 24-hour early warning, 72-hour notification, 14-day final report on actively exploited vulnerabilities, with the parallel track for severe incidents. Our incident playbooks are being aligned to the ENISA single reporting platform ahead of the September 2026 deadline.

Implementation Guidance for Distributors

Distributors share responsibility for keeping non-compliant product off the EU market. The CRA puts a clear obligation on distributors to verify that products bear the CE marking, are accompanied by the required documentation, and come from a manufacturer that meets its CRA obligations. Here is what MultiTech recommends and what we provide to make this straightforward.

What MultiTech provides

- EU Declaration of Conformity, CE marking, and updated technical documentation per product family, available on request and on the product page.
- Security advisories and PCNs distributed through our standard partner channels.
- Documented support and update lifetime per product family, in line with the CRA's minimum five-year support requirement.

- Direct CSIRT contact for any vulnerability or incident a distributor needs to escalate on behalf of an end customer.

What we ask distributors to do

- Stock and resell only product with current CE marking and supporting documentation. Devices manufactured before 1 August 2025 remain saleable under the prior regime; new stock should be confirmed as RED-DA compliant.
- Forward security advisories to your customers promptly. Subscribe at multitech.com/security/ to be notified when new advisories are published.
- Route any customer-reported vulnerability or incident to MultiTech's security contact within 24 hours so we can meet our CRA reporting clock.
- Keep records of which products went to which end customers — this supports both warranty and the CRA traceability expectation.

Implementation Guidance for End Customers and Integrators

If you are deploying MultiTech gateways or routers into a larger solution, compliance is shared. MultiTech is responsible for the device-level controls; you are responsible for how the device is configured, integrated, and operated in your environment. The steps below describe what to do to inherit MultiTech's compliance work cleanly.

At commissioning

- Set a strong, unique password at first boot. The minimum length on commissioned devices is 15 characters; longer is better.
- Disable any interfaces or services you do not need. Leave the factory-default minimums in place wherever possible.
- Enroll the device in DeviceHQ (or your equivalent management system) so update and configuration state is centrally visible.
- Where the application allows, use TPM-backed identity (AP300-class devices) and certificate-based authentication rather than shared secrets.

During operation

- Keep firmware current. Subscribe to multitech.com/security/ for advisories and apply security-critical updates within the window indicated in the advisory.
- Export device logs to your enterprise log management system (syslog supported) so security-relevant events are retained off-device.
- For deployments handling personal data, configure encryption at rest and in transit at the application layer — MultiTech provides the cryptographic building blocks (OpenSSL, TLS, LoRaWAN-native encryption), but the data-handling policy is yours.
- Maintain physical security of installations. MultiTech devices are not tamper-resistant by design; the installation environment must be.

If you discover a vulnerability

- Report it through multitech.com/security/ or to your MultiTech sales contact. We acknowledge reports promptly and triage under our CSIRP.
- For actively exploited vulnerabilities, MultiTech will issue an advisory within the CRA timeline; integrators are expected to apply the fix and notify their own downstream users.

MultiTech's Ongoing Security Posture

Product compliance only works if the company behind it is itself secure. MultiTech evaluates its systems and processes against the NIST Cybersecurity Framework (CSF) and maintains:

- 24/7 Managed Detection and Response (MDR) coverage.
- Continuous vulnerability scanning across corporate and manufacturing networks.
- Cybersecurity insurance with enforced multi-factor authentication.
- Security Awareness Training (SAT) for all employees.
- SOC 2 audited controls for customer data; ISO 27001-aligned information security roadmap.
- Air-gapped manufacturing networks separated from enterprise systems.
- A dedicated Cybersecurity Incident Response Team (CSIRT) that monitors and aligns with NIST, MITRE CVE, the EU Cyber Resilience Act, the UK PSTI Act, California AB 1906, and ANATEL Act 77 in Brazil.

Appendix: NISTIR 8228 Capability Reference

For integrators evaluating MultiTech IoT gateways and routers against the U.S. NIST framework for IoT cybersecurity (NISTIR 8228), the table below summarizes platform-level capabilities by category. It complements — and does not repeat — the RED-DA, CRA, and implementation guidance above. Specific behavior may depend on the product family and the active mPower release; consult product documentation or your MultiTech contact for the definitive list.

NISTIR 8228 Area	Capability Focus	MultiTech Gateways & Routers — What's Available
Asset Management	Unique device ID, enterprise asset integration, dependency disclosure	Unique identifier provisioned at device birth or by the user — managed in TPM 2.0 on AP300-class hardware, open memory on other models. DeviceHQ client interfaces with public or private cloud-based asset management for visibility and configuration. External software dependencies — firmware images, DeviceHQ service, LoRa network server — are documented for integrators.
Vulnerability Management	Scanning, identification, reporting	Penetration testing, binary analysis, and CVE triage performed by MultiTech and third parties. Centralized enterprise vulnerability systems can interface via MultiTech firmware APIs — contact MultiTech for the integration specification. No on-device vulnerability scanner runs by default, to preserve compute headroom for user applications.
Access Management	Identity, least privilege, lockouts, tamper	Unique identifiers for users, the device itself, and CPU processes (device-id, TPM, self-signed certificates). Custom roles and personas; TOMOYO and MAC security for process-level confinement. Password characters concealed on entry. Configurable lockout thresholds and idle-session timeouts. Physical tamper resistance is the integrator's responsibility — installations must be

NISTIR 8228 Area	Capability Focus	MultiTech Gateways & Routers — What's Available
		physically secured.
Incident Detection	Logging, SIEM integration, incident analysis	Security-relevant events written at appropriate syslog levels. Logs are exportable to enterprise SIEMs; MAC-violation logging is supported. Native intrusion-detection or anti-malware integration is not provided on-device — incident analysis is supported externally via the exported log stream.
Data Protection	Storage, transit, and backup	User-data encryption available with or without a hardware root of trust, depending on platform. Root filesystem is read-only; factory reset sanitizes the overlay and returns the device to a known state. Configuration backup and restore via DeviceHQ download or user-defined defaults. LoRaWAN is inherently encrypted; OpenSSL provides current cryptography for TLS-based protocols.
Privacy	PII handling and federated identity	MultiTech devices do not themselves collect or store personally identifiable information, so PII policy and information-flow controls remain with the integrator at the application layer. RADIUS supports federated identity for non-local users.

Looking Forward

December 11, 2027 is the date every connected-product manufacturer in the EU market is now working toward. By then, the Cyber Resilience Act will require evidence of secure design, vulnerability handling, SBOM management, secure updates across a documented support period, conformity assessment, and rapid incident reporting for every product placed on the market. MultiTech's view is that this should not be a sprint at the deadline — it should be the way connected products are built and supported every day.

Our roadmap is straightforward. RED-DA conformity is in place today, and CE-marked product is shipping. CSIRP playbooks are being aligned to the ENISA single reporting platform ahead of the September 11, 2026 reporting obligations. SBOM coverage and secure-update tooling are being deepened across the mPower platform and our hardware families. Where future product features touch the CRA's Critical Class I or II categories, we will engage Notified Bodies early so distributors and customers never face an unexpected conformity gap.

None of this is something MultiTech does in isolation. Our distributors are the front line of EU market access; our integrators are responsible for how our products land in real deployments. The technical building blocks are ours to provide — the operational discipline of keeping firmware current, documentation organized, and incidents reported promptly is a shared responsibility. We are committed to being the partner that makes that shared responsibility easy to carry.

If you have questions about your specific product family, your distribution program, or your integration plan, please reach out — we would much rather have the conversation early than at a deadline.

CONNECT WITH MULTITECH

World Headquarters — USA · +1 (763) 785-3500 · sales@multitech.com
EMEA — UK · +44 (0)118 959 7774 · sales@multitech.co.uk
Multi-Tech Systems, Inc., 2205 Woodale Drive, Mounds View, MN 55112 U.S.A.

Security advisories: multitech.com/security/ · **Support:** multitech.com/support/ · **Web:** multitech.com

Document 86003004 · 05-2026