Milesight LoRaWAN Gateway - EU Cyber Resilience Act (CRA) Readiness

1. Introduction

The EU Cyber Resilience Act (CRA, Regulation (EU) 2024/2847) establishes horizontal cybersecurity requirements for products with digital elements placed on the EU market. It entered into force on 10 December 2024, with full applicability from 11 December 2027.
This document describes Milesight's CRA readiness posture for its LoRaWAN gateway product family, outlines the security measures already in place, and summarizes our compliance roadmap.

1.1 Applicable Products

Model	Type
UG65	8-Channel LoRaWAN Gateway
UG67	8-Channel LoRaWAN Gateway (Outdoor, IP67)
UG56	8-Channel LoRaWAN Gateway
UG63	8-Channel LoRaWAN Gateway
EG71	Building IoT Gateway (Multi-Protocol)
SG50	Low-Power LoRaWAN Gateway (Outdoor)

1.2 Regulatory Context

Regulation	Scope	Milesight Status
CRA (EU) 2024/2847	Cyber resilience for products with digital elements	Compliance roadmap in progress (deadline: Dec 2027)

RED Delegated Act (EU) 2022/30	Cybersecurity for internet-connected radio equipment	EN 18031-1/-2 certified (certificates obtained)

RED-DA EN 18031 certification covers secure default configuration, access control, data confidentiality, communication security, and privacy protection - requirements that **align closely with** CRA Annex I and **can support compliance**. Data Act and GDPR disclosures are listed in Section 13 - Related Documents.

2. Regulatory Timeline

Date	Milestone	Status
2024.12.10	CRA enters into force	Effective
2026.06.11	Conformity assessment provisions apply	Effective
2026.09.11	Vulnerability reporting obligations (Article 14)	Upcoming
2027.12.11	Full CRA applicability	Upcoming

Milesight's internal compliance roadmap is described in Section 12.

3. Product Classification

Milesight LoRaWAN gateways are currently classified as **default class** products under the CRA, supporting the internal-control conformity assessment route (Module A).

Rationale: LoRaWAN gateways perform protocol-level data forwarding between LoRa RF networks and IP networks. They do not operate network-layer routing protocols (OSPF, BGP, RIP) that characterize traditional routers as defined in Annex III Part I. This classification aligns with industry practice among comparable gateway manufacturers. If official EU guidance reclassifies gateway products, Milesight will reassess and adjust its conformity assessment route accordingly.

4. Security Foundations

CRA compliance builds on existing security controls validated through third-party testing.

4.1 EN 18031 Cybersecurity Certification

All Milesight LoRaWAN gateways have been assessed against harmonised standards under the RED Delegated Act:

Model	EN 18031-1 (Network Security)	EN 18031-2 (Privacy Protection)	EU-Type Examination
UG65 / UG67	Certified	Certified	RED-3912
UG56	Certified	Certified	RED-3911
EG71	Certified	Certified	RED-4209
SG50 / UG63	Certified	Certified	RED-4096

Notified Body: SGS Fimko OY (NB 0598)

4.2 Organizational Certifications

Certification	Standard	Scope
ISO/IEC 27001:2022	Information security management	Organizational ISMS
ISO 9001:2015	Quality management	Design, manufacturing, sales

4.3 Additional Compliance

- **UK PSTI Act**: Statement of compliance published (https://www.milesight.com/legal/psti-statement-of-compliance.pdf)
- **NIS2 Directive**: Alignment statement published (https://resource.milesight.com/milesight/iot/document/milesight-iot-nis2-statement.pdf) - CRA addresses product-level cybersecurity; NIS2 addresses organizational-level service continuity. The two are complementary (CRA Recital 81).

- **GDPR**: Privacy-by-design guideline published (https://resource.milesight.com/milesight/iot/document/milesight-lorawan-gateway-privacy-data-protection-guideline.pdf)

5. Product Security Measures

The security measures below address the product security attributes of CRA Annex I Part I. Vulnerability handling requirements (Annex I Part II) are covered in Section 6 and Section 7.

CRA Annex I Part I Requirement	**Whitepaper Section**
(1) Risk-proportionate cybersecurity in design, development, and production	4 Security Foundations, 12 Roadmap
(2)(a) No known exploitable vulnerabilities	6.2 Security Testing
(2)(b) Secure default configuration	5.1
(2)(c) Secure update mechanism	6.3
(2)(d) Access control and authentication	5.2
(2)(e) Data confidentiality	5.3
(2)(f) Data and configuration integrity	5.1, 5.3
(2)(g) Data minimization	5.3
(2)(h) Functional availability (DoS mitigation)	5.4
(2)(i) Minimize negative impact on connected devices	5.3
(2)(j) Minimize attack surface	5.1

(2)(k) Reduce incident impact	5.4
(2)(l) Security monitoring and logging	5.5
(2)(m) Secure data deletion and migration	5.1

5.1 Secure by Design and Default

- **First-access password enforcement**: Default credentials are invalidated after first login - users must set a strong password meeting configurable complexity requirements before gaining full access
- **Secure default configuration**: Unnecessary services disabled by default (e.g., Telnet off)
- **Factory reset**: Physical button, Web UI, and remote management interfaces (HTTP API, SSH, MDP)
- **Firmware integrity**: Digitally signed firmware with automatic signature verification

5.2 Access Control and Authentication

- **Credential protection**: bcrypt password hashing with configurable complexity
- **Role-based access**: Admin and Viewer roles with differentiated permissions
- **Session management**: Automatic session timeout
- **Secure remote access**: HTTPS for Web UI, SSH for CLI

5.3 Data Protection

- **Transport encryption**: TLS 1.2/1.3 for MQTT, HTTPS, and cloud connections
- **LoRaWAN security**: AES-128 encryption at network and application layers with MIC integrity
- **Data minimization**: No telemetry or data transmitted to Milesight by default
- **Network isolation**: Configurable firewall with WAN-zone default-reject policy

5.4 Resilience and Availability

- **DoS protection**: SYN flood protection enabled; rate limiting on web services
- **Service isolation**: Optional Docker container isolation (EG71/UG6X) with security controls aligned with CIS Docker Benchmark - privilege escalation prevention, namespace isolation, sensitive path protection, and audit logging
- **Offline resilience**: Data buffering during network outages with automatic retransmission

5.5 Security Monitoring

- **System logging**: Login events, configuration changes, security events
- **Log integrity**: Tamper-evident log rotation
- **Remote forwarding**: Configurable syslog forwarding to external collectors

6. Vulnerability Management

6.1 Vulnerability Disclosure Policy

Milesight operates a Vulnerability Disclosure Policy (VDP):

- **Reporting channel**: https://www.milesight.com/legal/vulnerability-report
- **Contact**: security@milesight.com
- **Response commitment**: Acknowledgment within 5 business days
- **Safe harbor**: No legal action against researchers who act in good faith and follow responsible disclosure practices

6.2 Security Testing

Security testing runs before each product release:

- **Static code analysis**: Automated scanning of source code for security defects
- **Vulnerability scanning**: Multi-tool assessment (web application, network, and host scanning)
- **Component analysis**: Identification of known vulnerabilities in third-party dependencies
- **Remediation**: Critical and high issues fixed before release; lower severity triaged on risk

6.3 Security Updates

- **Free of charge**: Security updates provided at no cost during the product support period
- **Signed delivery**: All firmware updates are digitally signed and verified before installation
- **Multiple channels**: Over-the-air via Milesight Development Platform (MDP), or manual download
- **Release notes**: Security-relevant changes documented in product release notes (https://www.milesight.com/support/resources/firmware#lorawan-gateway)
- **Customer notification**: Release notes published on milesight.com; customers enrolled in Milesight Development Platform (MDP) receive firmware update notifications

6.4 CVE History

Milesight has a track record of coordinated vulnerability disclosure with external researchers and government agencies (including CISA). All identified vulnerabilities have been remediated within the affected product's support period.
Full advisory details: https://www.milesight.com/resources/support/security-vulnerability-management

7. Software Bill of Materials (SBOM)

Milesight maintains an internal SBOM for each product, identifying software components and dependencies in a commonly used, machine-readable format as required by CRA Annex I Part II(1). The SBOM is used to:

- Cross-reference components against known vulnerability databases (MITRE CVE, upstream advisories)
- Drive patch decisions during the product support period
- Support Article 14 vulnerability reporting obligations

SBOMs are available to market surveillance authorities upon request.

8. Implementation Guidance for Distributors

Distributors share CRA responsibility under Article 20: only compliant products should be placed on the EU market. The CRA requires distributors to verify CE marking, required documentation, and that the manufacturer meets its obligations.

What Milesight Provides

- **EU Declaration of Conformity** and CE marking documentation for each product family, available on request
- **Security advisories** published at milesight.com/resources/support/security-vulnerability-management
- **Firmware updates** with security-relevant changes documented in release notes (https://www.milesight.com/support/resources/firmware#lorawan-gateway)
- **Direct security contact** (security@milesight.com) for any vulnerability or incident that requires escalation
- **Documented support periods** per product family

What We Ask Distributors to Do

- **Verify CE marking**: Products placed on the EU market after 11 December 2027 must carry the CE marking and be accompanied by the required documentation. Products already placed on the market before this date are subject to the transitional provisions of CRA Article 69
- **Forward security advisories**: Subscribe to Milesight security notifications and pass advisories to customers
- **Route vulnerability reports**: Forward any customer-reported vulnerability or security incident to security@milesight.com promptly so Milesight can meet its CRA Article 14 reporting obligations
- **Cooperate with authorities**: Be prepared to provide product compliance information to market surveillance authorities upon request, as required under CRA Article 20

9. Implementation Guidance for Integrators and End Customers

Milesight is responsible for delivering a secure product; secure deployment depends on proper configuration and operation. The following recommendations help integrators and end customers maximize their security posture.

At Commissioning

- **Set a strong, unique password** at first boot - Milesight devices enforce password setup at initial access
- **Disable unnecessary interfaces**: Leave the factory-default minimum service configuration in place wherever possible
- **Enroll in MDP** (Milesight Development Platform) for centralized firmware visibility and update management
- **Configure TLS**: Use certificate-based authentication for MQTT and HTTPS connections where the application allows

During Operation

- **Keep firmware current**: Monitor Milesight security advisories and apply security-critical updates promptly
- **Export logs**: Forward device logs to your enterprise SIEM via syslog so security-relevant events are retained off-device
- **Protect personal data**: Milesight provides cryptographic building blocks (TLS, LoRaWAN AES-128) - we recommend configuring encryption at rest and in transit at the application layer to meet your data-handling requirements
- **Maintain physical security**: Physical security is a prerequisite for device security - any device is vulnerable to destruction or tampering if an attacker has unrestricted physical access. Ensure the installation environment provides appropriate physical controls (locked enclosures, access control, surveillance)

If You Discover a Vulnerability

- Report it through https://www.milesight.com/legal/vulnerability-report or security@milesight.com
- Milesight operates a Safe Harbor policy - no legal action against good-faith researchers
- For actively exploited vulnerabilities, Milesight will issue an advisory within the CRA timeline; integrators are expected to apply the fix and notify their own downstream users

10. Article 14 Reporting Readiness

CRA Article 14 requires reporting actively exploited vulnerabilities and severe incidents to ENISA and designated CSIRT coordinators. Internal procedures for vulnerability classification, escalation, regulatory reporting, and evidence preservation are documented ahead of September 2026:

Requirement	Timeline	Preparation Status
Early warning notification	Within 24 hours	Procedure documented
Initial notification	Within 72 hours	Procedure documented
Final report	Within 14 days	Procedure documented

11. Support Period

Milesight provides security updates for a minimum of **5 years** from the date each product is first placed on the EU market, in accordance with CRA Article 13(8). End-of-support dates (month and year) for each product model are published in product documentation and on milesight.com.

12. CRA Compliance Roadmap

Phase	Timeline	Focus
Phase 1	Q3 2026	Third-party penetration testing
Phase 2	Q4 2026	EU Declaration of Conformity
Phase 3	Q2 2027	Third-party CRA conformity assessment
Phase 4	Q3 2027	CE marking update, formal CRA compliance declaration

Completed Milestones

- EN 18031-1/-2 cybersecurity certification (all product families, SGS NB 0598)
- Vulnerability Disclosure Policy published
- Security advisory page published
- PSIRT established with Article 14 reporting procedures (24h/72h/14d to ENISA)
- Internal SBOM process established
- Product security self-assessment against CRA Annex I Part I (a)-(m) completed

13. Related Documents

Document	Location
Trust Center	https://www.milesight.com/company/trust-center

Security Advisories	https://www.milesight.com/resources/support/security-vulnerability-management
Vulnerability Disclosure Policy	https://www.milesight.com/legal/vulnerability-report
Vulnerability Report	security@milesight.com
GDPR Guideline	https://resource.milesight.com/milesight/iot/document/milesight-lorawan-gateway-privacy-data-protection-guideline.pdf
EU Data Act Transparency Statement	https://resource.milesight.com/milesight/iot/document/milesight-lorawan-gateway-eu-data-act-product-data-disclosure-applicability-statement.pdf
NIS2 Alignment Statement	https://resource.milesight.com/milesight/iot/document/milesight-iot-nis2-statement.pdf
UK PSTI Statement	https://www.milesight.com/legal/psti-statement-of-compliance.pdf
EN 18031 Certificates	Available on request
Firmware Downloads	https://www.milesight.com/support/resources/firmware#lorawan-gateway

14. Contact

Purpose	**Contact**
Security Vulnerability Reports	security@milesight.com
Product Support	https://www.milesight.com/support/technical-support
General Inquiries	https://www.milesight.com/company/contactus

Readiness posture as of July 2026. Compliance activities are ongoing - this document will be updated as milestones are achieved. A formal EU Declaration of Conformity will be published upon completion of the conformity assessment process.