



MYC-JR3576 Security Vulnerability Remediation and CRA Compliance Support

Document Type	Technical Statement / Compliance Support
Applicable Platforms	MYC-JR3576
Document Version	V0.9
Issued By	MYIR Electronics Limited

[Make Your Idea Real](#)

Web: en.myir.cn | Mail: sales@myir.cn | Tel: +86-755-22984836



1 Security Vulnerability Remediation Scope

This document explains, for customers planning to place final products on the EU market, the MYIR system-on-module and Linux BSP capabilities and processes in the following areas: security vulnerability remediation, security issue response, static security scanning, CRA compliance support and ongoing maintenance.

1.1 Objects Covered

MYIR security vulnerability remediation covers the complete Linux BSP software stack delivered by MYIR:

1. Linux kernel (including drivers and security subsystems)
2. U-Boot bootloader
3. OP-TEE trusted execution environment (where enabled on the platform)
4. BSP packages, user-space libraries and middleware in the root file system
5. Third-party open-source components integrated, built and validated by MYIR

MYC-JR3576 platform notes

- Objects covered: U-Boot with secure FIT, OP-TEE, Linux kernel (6.1.141), user space and middleware
- SDK: L6.1.141 V1.0.0; sources are delivered under 04-Sources
- **The release package ships security material:** SoftwareFiles/Patch/security/ — the Security Application Note V1.0 plus the target security patch set (luksmeta, rockchip-tee-user-app, secure_fit, ota-cms, etc.)

1.2 Ownership and Division of Responsibility

- **MYIR is responsible for:** vulnerability investigation, assessment and remediation of the components contained in the BSP it delivers, delivered as a security update (OTA) or a version release.
- **The customer is responsible for:** remediation of vulnerabilities in application software, business logic and code developed, integrated or deployed by the customer. MYIR provides remediation methods and interface guidance.

1.3 Basis for Remediation

- Sources: vendor advisories, the CVE database (NVD), upstream patches and public information from security research organisations.
- Process: the exploitability and impact of each vulnerability under MYIR's default configuration are assessed before remediation.
- Marking: components that are not enabled or not reachable in the current BSP version are explicitly marked with their affected status in the VEX report.

1.4 Remediation Artifacts

1. **Security update (OTA):** an A/B partition scheme based on an OTA solution (RAUC, SWUpdate, Mender, etc.) with signature verification and automatic rollback on failure.
2. **Version release:** complete fixes shipped with a new BSP release.

3. **Standalone security patch:** security fixes can be separated from feature updates and delivered independently.

1.5 Support Period

- MYiR provides security vulnerability remediation only for BSP versions within the support period.
- Support duration and the version policy are described in Chapter 5; for versions past the support period MYiR provides upgrade and migration guidance.

2 Security Issue Response Mechanism

To meet the CRA requirements for vulnerability management and incident response (the EU vulnerability reporting obligation applies from 11 September 2026), MYiR has established a Product Security Incident Response Team (PSIRT).

2.1 PSIRT Responsibilities

- Receiving and acknowledging security vulnerability reports
- Vulnerability impact assessment
- Defining and executing the remediation plan
- Publishing security advisories and VEX reports
- Sharing security information with customers

2.2 Reporting Channel

- **Where to report:** the **PSIRT** page in the MYiR Developer Center — developer.myr.cn/user/security.html. That page publishes the reporting e-mail, the PSIRT scope and workflow, security advisories and the **PGP public key**.
- **Obtain the reporting mailbox from that page.** In addition, **every vulnerability report must be encrypted with the MYiR PSIRT PGP public key published there before it is sent — never send a report unencrypted** (vulnerability details are sensitive and an unencrypted e-mail may leak them).
- **How to encrypt:** import that PGP public key with a tool such as OpenPGP / GnuPG and encrypt the report; e-mail built-in plugins and S/MIME are **not recommended**, and passphrases, symmetric encryption or passwords should **never** be used.
- **Suggested content:** contact details (name, contact information, location, company, position); affected product model and software/hardware versions, how the issue was found, reproduction steps, impact description and on-site handling; attachments (full vulnerability report, logs, screenshots, remediation suggestions).

2.3 Response Timeframe (SLA)

Stage	Time	Description
Initial alert	Within 24 hours	Acknowledge the report, give a preliminary assessment and receipt
Detailed notification	Within 72 hours	List of affected components and versions, preliminary impact analysis
Remediation report	Within 14 days	Remediation plan, mitigations and update schedule

2.4 Vulnerability Assessment and VEX Disclosure

MYIR follows a coordinated vulnerability disclosure (CVD) policy, assesses exploitability and impact, and issues VEX reports in accordance with the CycloneDX VEX specification.

VEX status	Meaning
Not Affected	Not exploitable under the default BSP configuration (the vulnerable module is not enabled)
Under Investigation	Assessment in progress
Fixed	Fixed in the current version
Affected	Confirmed exploitable; upgrade or mitigation required immediately
False Positive	Scanner false positive (version match but the patch is already merged)

3 Handling of Static Security Scan Results

Static security scanning identifies potential security defects in BSP source code and open-source components (mapped to CWE categories). It complements manual audit and vulnerability management and can be performed with tools such as CodeQL.

3.1 Position and Scope of Scanning

- Position: one of the static analysis inputs to the vulnerability management process.
- Scope: semantic-level defect detection for C/C++ components and key sources inside the BSP.
- Detects: buffer overflows, injection, out-of-bounds access, unsafe dereferences and similar defect classes.

3.2 Review of Results

MYIR reviews scan results supplied by customers item by item and decides whether each alert constitutes a real, exploitable vulnerability, based on:

1. Component version and origin
2. Call path and reachability
3. Mitigations present in the default configuration
4. False-positive identification (version match with the patch already merged, unreachable code, and so on)

3.3 Classification and Disposition

- Confirmed issues enter a single vulnerability tracking process by risk level (high / medium / low).
- Results are merged and prioritised together with CVE scanning (cve-check) and VEX analysis.
- High-risk issues are handled first.

3.4 Closing the Loop

- Confirmed issues are fixed through BSP security updates and re-verified in subsequent versions.
- The output of a single tool is never the final verdict; static scanning, CVE monitoring, manual audit and VEX analysis together form a closed loop.

4 Support for CRA Requirements

The EU Cyber Resilience Act (CRA), **Regulation (EU) 2024/2847**, establishes horizontal cybersecurity requirements for products with digital elements placed on the EU market and imposes lifecycle security requirements on manufacturers. Relevant cybersecurity standards, including IEC 62443 where applicable, may support implementation and assessment; **IEC 62443 is not itself the legal basis of the CRA.**

4.1 CRA Timeline

Date	Event	Impact
2024-12-10	CRA enters into force	The regulation is in force; start compliance preparation
2026-09-11	Vulnerability reporting obligation applies	A PSIRT and a vulnerability reporting process are required
2027-12-11	Full application	All products placed on the EU market must be fully compliant

4.2 Key CRA Requirements

1. Secure by default and secure by design: default security configuration, minimised attack surface, no weak credentials and no unnecessary open ports
2. Software bill of materials (SBOM): a machine-readable component inventory
3. Vulnerability management and incident response: discovery / assessment (VEX) / remediation / reporting, plus a PSIRT
4. Security updates (OTA): provided continuously during the support period and protected by signature and integrity verification
5. Technical documentation and risk assessment: security architecture documentation and a TARA risk assessment report

4.3 Four Compliance Mechanisms and Corresponding Capabilities

Mechanism	Description	Benefit to the customer
Automatic SBOM generation	Yocto create-spdx produces SPDX (machine-readable JSON), converted to CycloneDX by script; covers the whole image / rootfs / recipes / packages — kernel, U-Boot, BSP packages and user space	No toolchain to build; the result imports directly into vulnerability scanners
CVE monitoring + VEX	cve-check matches NVD automatically; High / Critical findings receive manual VEX analysis	The VEX report can be used directly in compliance filing
PSIRT response	Handled through the PSIRT page in the MYIR Developer Center (see Chapter 2); 24 h alert → 72 h notification → 14 day report	Meets the CRA vulnerability reporting obligation
Security update (OTA)	RAUC / SWUpdate etc. (A/B partitions + signature verification, tamper and rollback protected)	Patches deploy directly; at least 5 years of free security updates
Compliance documents	TARA risk assessment / security architecture document / CVD policy / declaration templates	Reuse of document templates

4.4 IEC 62443-4-2 Product-Level Security Implementation

IEC 62443-4-2 defines component-level (SL-C) technical security requirements covering identification and authentication control (IAC), use control (UC), system integrity (SI), data confidentiality (DC), restricted data flow (RDF), timely response to events (TRE) and resource availability (RA). MYIR provides concrete implementation for four areas: **secure boot, secure storage, secure update and access control**.

Each subsection below adds the platform-specific implementation and document sections for the Rockchip platform (MYC-JR3576) on top of the generic capability.

4.4.1 Secure Boot

- Root of trust: the public key hash (SRK / ROTPK) stored in on-chip OTP, verifying bootloader and kernel signatures step by step
- Chain of trust: BootROM → Loader/SPL → OP-TEE → U-Boot → boot.img (kernel/DTB); boot stops if any stage fails verification
- Trusted execution environment: OP-TEE based on ARM TrustZone
- Anti-rollback: OTP version counters / eFuse counters prevent downgrading to an older firmware version

MYC-JR3576 implementation

- **Implementation guide:** SoftwareFiles/Patch/security/MYD-JR3576 Security Application Note-V1.0.pdf — §3 **Safe Start** (boot flow / building the secure boot image / principles)
- Mechanism: Rockchip secure boot (**U-Boot secure FIT** + step-by-step verification + OTP)
- **Deliverables:** the secure-boot configuration patches in Patch/security/ (rockchip_ub_secure_fit.config and others) and a ready-to-apply U-Boot configuration; following the document steps produces the signed boot image

4.4.2 Secure Storage

- Secure storage medium: RPMB (hardware replay and rollback protection in eMMC)
- Key management: encryption keys are managed by a key-management trusted application (TA/ KeyBox) inside OP-TEE and never appear in normal-world memory in plaintext
- System integrity: dm-verity provides block-level integrity verification of read-only system partitions; dm-crypt provides transparent partition encryption
- Cryptography: AES, RSA, SHA and a hardware true random number generator (TRNG)

MYC-JR3576 implementation

- **Implementation guide:** SoftwareFiles/Patch/security/MYD-JR3576 Security Application Note-V1.0.pdf — §4 **system security** (§4.2 DM, §4.3 system verification, §4.4 system encryption)
- Mechanism: **dm-verity** (system verification) + **dm-crypt** (system encryption) + ramdisk
- **Hardware root of trust: onboard TPM 2.0** (listed in the MYC core board product manual's on-board device list), usable for secure key storage and platform integrity measurement

- **Deliverables:** security patch set in Patch/security/ (luksmeta and related components) plus the verification / encryption image build steps of §4

4.4.3 Secure Update / OTA

- Signature verification: the update image is signed and is written only after verification succeeds
- Integrity check: the update package carries a checksum, preventing man-in-the-middle injection
- A/B partitions + rollback: automatic rollback when an update fails; key subsystems can be updated independently
- Support commitment: **at least 5 years** of free security updates; security patches can be pushed independently

MYC-JR3576 implementation

- **Implementation guide:** SoftwareFiles/Patch/security/MYD-JR3576 Security Application Note-V1.0.pdf — §6 Security Upgrade (§6.1 CMS, §6.2 signed images, §6.3 secure OTA upgrade)
- Mechanism: signed OTA (CMS)
- **Deliverables:** the OTA verification component patch (Patch/security/, ota-cms-verify) plus the signing, packaging and update scripts; §6 walks the customer through a complete secure OTA

4.4.4 Access Control (Mandatory Access Control / AppArmor)

- Mechanism: Linux LSM mandatory access control (AppArmor) that grants access per process profile, **entry by entry — anything not listed is denied**
- Complements DAC: even when a service runs as root, a compromised service can only touch the resources listed in its profile (permissions travel with the program, not with the file)
- Policy persistence: profiles live in /etc/apparmor.d/ and are loaded automatically at boot by apparmor.service; a **path-attached** profile confines plain execution with no extra interaction
- Two modes: **enforce** (blocking) and **complain** (log only, for pre-production tuning)
- Auditing: denials are written to the systemd journal (query with journalctl)

This addresses the use control (UC) and identification and authentication control (IAC) requirements of IEC 62443-4-2, as well as the CRA access-control and least-privilege expectations.

MYC-JR3576 implementation

- **Implementation guide:** Chapter 4.4.4 of this document (mechanism, modes and persistence)
- The current SDK **does not enable MAC by default** (the Patch/security/ patch set contains neither AppArmor nor SELinux)
- Where access control is required, MYIR ports the approach already proven on i.MX95 (kernel LSM + AppArmor user space + policy set) to this platform and adapts the profiles for the image

- **Deliverables:** kernel LSM configuration and apparmor user-space packages plus the adapted on-device policy set (/etc/apparmor.d/), shipped with the image once enabled

4.5 Platform SBOM Support

For the platform in use, MYIR runs a complete SBOM generation and delivery process that feeds directly into the customer's CRA compliance filing; the process does not depend on the SoC vendor:

1. **Format: SPDX (machine-readable JSON, *.spdx.json)**, satisfying the CRA requirement for a machine-readable SBOM; **CycloneDX** output is available on request
2. **Generation:** produced automatically by Yocto create-spdx during the BSP build, written component by component by the build system, with no manual compilation and always in step with the firmware image
3. **Coverage:** issued layer by layer — whole image → rootfs → each recipe → each package; including **U-Boot, the Linux kernel (with modules and device trees), TF-A, OP-TEE and BSP packages**, plus all user-space libraries and middleware in the rootfs, covering the in-house and third-party components the CRA looks for
4. **Fields:** component name, version, supplier, licence, file checksums, the mapping between sources and binaries and the relationships between components, all recorded per the SPDX specification
5. **Delivery:** each SBOM corresponds one-to-one to a firmware version and is issued together with every image and security patch release; customers may also request the SBOM of any specific version, and MYIR keeps providing it throughout the support period
6. **Link to vulnerability status:** the SBOM itself is a component inventory and **carries no CVE / VEX fields**; vulnerability status is issued separately in MYIR's **CVE scan report and VEX report**, matched item by item against the SBOM components so that the customer can merge them directly into its own compliance file

The platform SBOM is a technical input to the customer's CRA compliance process; it does not by itself constitute final-product compliance, nor does it replace the assessment and documentation obligations of the final-product manufacturer.

MYC-JR3576 implementation

- **Implementation guide:** Chapter 4.5 of this document (complete description of the SBOM format, generation, coverage and delivery)
- **Generation:** enabling Yocto create-spdx during the BSP build produces the machine-readable JSON deliverables (*.spdx.json) under build-.../tmp/deploy/spdx/
- **Coverage:** issued layer by layer for whole image / rootfs / recipe / package, including U-Boot, the Linux kernel (with modules and device tree), BSP packages and rootfs user-space components, strictly matched to the firmware version
- MYIR issues the SPDX file for the firmware version the customer specifies and can convert it to CycloneDX on request; the SBOM carries no CVE / VEX fields, vulnerability status coming from the CVE scan report and VEX report matched item by item against the SBOM components

4.6 Customer Responsibilities and Incident Reporting

- The CRA imposes incident reporting obligations on products placed on the EU market.

- As the placer of the final product, the customer is responsible for reporting exploited vulnerabilities and serious security incidents to the relevant EU bodies (ENISA and the national CSIRT).
- As the component and module supplier, MYIR provides SBOMs, VEX reports, security advisories and vulnerability response capabilities to support the customer's compliance filing.

4.7 Platform CRA Capability Index (MYC-JR3576)

The table below gives, for each CRA capability: what MYIR provides, which document and section the customer follows to complete the implementation, and the **relative paths of the deliverables inside the SDK release package**. Paths start at the package root: 01-Docs (documents), 02-Images (pre-built images), 03-Tools (tools), 04-Sources (sources); a platform security directory is written out in full. \$SDK stands for the platform project root unpacked under 04-Sources; "build output" means the directory produced after building as documented; paths beginning with / are on-device (root filesystem) paths.

CRA capability	What MYIR provides	Implementation guide	Deliverables / SDK path
Secure Boot (chain of trust)	Rockchip secure boot: u-boot secure FIT + stage-by-stage verification + OTP public-key hash	<i>MYD-JR3576 Security Application Note</i> §3 Safe Start (SoftwareFiles/Patch/security/); Chapter 4.4.1 of this document	In the package: configuration patches such as SoftwareFiles/Patch/security/rockchip_ub_secure_fit.conf (same patch set) and the pre-built images under 02-Images/; build output: the signed uboot.img / boot.img built as documented
Secure execution environment (TEE / OP-TEE)	OP-TEE + the KeyBox secure key component	<i>MYD-JR3576 Security Application Note</i> §5 (§5.1 OP-TEE, §5.2 KeyBox)	Patch and sample application: rockchip-tee-user-app under SoftwareFiles/Patch/security/; the OP-TEE components ship in the image
Secure storage and encryption of keys and sensitive data (hardware root of trust + hardware crypto)	dm-verity system verification + dm-crypt / luksmeta system encryption + ramdisk + onboard TPM 2.0 + the RK3576 built-in crypto engine and TRNG	<i>MYD-JR3576 Security Application Note</i> §4 (§4.2 DM, §4.3 system verification, §4.4 system encryption); Chapter 4.4.2 of this document	Patches: luksmeta and related items under SoftwareFiles/Patch/security/ plus the verification / encryption image scripts; the tpm2-* stack and kernel crypto drivers ship in the image
Device identity / key binding	Non-secure / secure OTP one-time programmable area (device-	<i>MYD-JR3576 Security Application Note</i> §2 (OTPs and Secure Peripherals), §5.2	The OTP programming procedure and tool commands given in that document; sample and patches: rockchip-tee-user-app under

	unique keys and public-key hash) + KeyBox key loading		SoftwareFiles/Patch/security/
Secure update (OTA)	Signed OTA (CMS): the signed image is verified before the update is applied	<i>MYD-JR3576 Security Application Note</i> §6 (§6.1 CMS, §6.2 signed image, §6.3 secure OTA upgrade); Chapter 4.4.3 of this document	Patch: ota-cms-verify under SoftwareFiles/Patch/security/ plus the signing / packaging and upgrade scripts (the update server is built by the customer)
Access control (MAC)	Not enabled by default (the patch set contains no AppArmor / SELinux); MYIR provides the porting and policy adaptation using the solution already verified on the i.MX95 platform	Chapter 4.4.4 of this document	Kernel LSM configuration and apparmor user-space packages plus the adapted on-device policy set /etc/apparmor.d/ (delivered with the image once enabled)
SBOM (supply-chain transparency)	Yocto create-spdx produces machine-readable SPDX JSON ; CycloneDX conversion on request	Chapter 4.5 of this document	Build output: *.spdx.json under \$SDK/build-*/tmp/deploy/spdx/ (issued for the firmware version the customer specifies)
Vulnerability handling (CVE / VEX / PSIRT)	MYIR PSIRT receiving, assessment and disclosure process; CVE scanning and VEX reports mapped component by component to the SBOM	Chapter 2 of this document (the PSIRT page is given there)	Security advisories, VEX reports and security patch packages: delivered through MYIR's release channel (download link) with every version release / patch package, matching the version recorded in the SDK Release Note under 01-Docs/

5 Maintenance Strategy

5.1 Support Period

- MYIR's standard commercial policy provides **at least five years** of free security updates and fixes for products covered by that policy.
- **The CRA support period is product-specific:** it must reflect the expected use of the product, reasonable user expectations, the nature and intended purpose of the product and other applicable requirements. The five-year commercial commitment should therefore not be read as a universal CRA support-period determination.
- As required by the CRA, MYIR states the applicable support-period end date in the technical documentation (to at least month precision) and informs customers accordingly.

5.2 Update Method

- Security patches are delivered as **version releases or standalone patch packages**, downloadable from MYIR's release channel.
- Security updates are separated from feature updates and can be released independently, so that customers can schedule deployment in their own maintenance window.
- Under **Article 13(9) of Regulation (EU) 2024/2847**, each security update made available during the applicable support period must remain available after issuance **for at least 10 years**, or for the remainder of the support period, whichever is longer; customers should incorporate this into their product lifecycle and documentation planning.

5.3 Version Policy

- Security fixes are applied continuously to the latest BSP version and backported to affected versions still in support, subject to technical feasibility and component availability.
- For versions that have reached end of support, upgrade and migration guidance is provided.

5.4 Continued Vulnerability Response

- While a version is in support, the PSIRT receiving, assessment and disclosure process remains in place.
- Security advisories and VEX reports continue to be shared with customers.

5.5 Long-Term Support

- MYIR tracks the evolution of the CRA, IEC 62443 and related standards.
- The security capability and compliance documentation set (security architecture document, TARA, CVD policy, declaration templates) is extended progressively.

This is the platform-specific edition. Every capability is mapped to the document section to follow, the deliverables provided and the SDK paths; MYIR technical support assists with implementation on request.