Zoomlion Heavy Industry Science & Technology Co., Ltd.

中联重科股份有限公司

Product Cybersecurity Management System / 产品网络安全管理体系

Coordinated Vulnerability Disclosure Policy

协调漏洞披露政策 (PRE-2)

Document No. ZL-SEC-CVD-001 Version V1.2 Status: Controlled draft Date: 2026-08-18

Revision History

Version	Author	Date	Change description
V1.2	Central Research Institute	2026-08-18	prEN 40000-1-3 PRE-2 requirements

Control item	Content
Applicable organisation	Zoomlion Heavy Industry Science & Technology Co., Ltd. and related business units
Applicable products	See Zoomlion CRA-applicable product list
Operating body	Zoomlion Product Security Incident Response Centre
Advisory ID	ZL-SA-YYYY-NNN

0 References and acknowledgements

- ISO/IEC 29147:2018; ISO/IEC 30111:2019; ISO/IEC TR 5895:2022
- prEN 40000-1-3 PRE-2; Regulation (EU) 2024/2847 (CRA)
- ENISA (2022) Coordinated Vulnerability Disclosure Policies in the EU
- ZL-SEC-VHP-001; ZL-SEC-PSIRT-001; ZL-SEC-SCOM-001; ZL-SEC-COM-001; ZL-SEC-ART14-001

Zoomlion Product Security Incident Response Centre thanks researchers, supply-chain partners and standards organisations that report cybersecurity issues in Zoomlion products in a responsible manner. This policy is structured with reference to international CVD good practice.

Executive summary

This document is the official coordinated vulnerability disclosure (CVD) policy and external operating guide of Zoomlion Central Research Institute Product Security Incident Response. It sets out Zoomlion Heavy Industry Science & Technology Co., Ltd.'s strategy, processes and responsibilities for receiving, validating, remediating, releasing and disclosing security vulnerabilities related to equipment on the Zoomlion CRA-applicable product list. Internal vulnerability handling is described in ZL-SEC-VHP-001; statutory reporting obligations are described in the Article 14 procedures.

Key objectives

- Provide security researchers with clear reporting channels, format requirements and expected response times
- Standardise assessment and remediation so that reports receive consistent, auditable handling and hand off into the VHP
- Through coordinated disclosure, limit public release of exploit details before a fix is available, protecting users in the field and the safety of field operations
- Provide a good-faith-research safe harbour within applicable law
- Meet prEN 40000-1-3, ISO/IEC 29147/30111/TR 5895 and CRA CVD requirements
- Close the security feedback loop and continually improve product security

Important notes

- A named owner follows up on valid reports; the security mailbox responds within 3 working days
- Severity levels are Critical / High / Medium / Low. Remediation targets follow the VHP by vulnerability risk (typically Critical/High/Medium ≤ 90 working days; Low ≤ 180 working days; stricter internal high-priority SLAs prevail)
- Publishing technical vulnerability details requires Zoomlion's written permission, or the non-disclosure period to have expired with PSIRT notified
- Good-faith research that complies with this policy is covered by the Annex C safe harbour
- Public vulnerability intake channel: vsoc_wlaq@zoomlion.com

Part I — Introduction

1.1 Introduction to coordinated vulnerability disclosure

Coordinated vulnerability disclosure is not a one-off event. It is an ongoing, multi-party process covering discovery, reporting, validation, remediation, release and public disclosure. CVD is iterative (the same issue may be validated more than once), collaborative (it depends on trust and communication), dynamic (the threat landscape changes priorities) and learning-oriented (cases feed improvement).

1.2 Background and terminology

1.2.1 Vulnerability

A vulnerability is an exploitable weakness in items on the CRA-applicable product list, or in supporting software/interfaces directly related to their security. It may exist in hardware, firmware, protocols, configuration, OTA, cloud services or third-party components. In essence: an unintended defect that can be used to violate a security policy and may harm confidentiality, integrity or availability, or affect the operational safety of construction machinery.

1.2.2 Exploit code, malware and security incidents

Exploit code is a method that produces unintended behaviour. Malware is software intended to damage or steal. A security incident is an actual or suspected violation of a security policy. Zoomlion Product Security Incident Response leads vulnerability response. When a vulnerability intersects an in-the-wild incident, PSIRT coordinates with VSOC/incident response and assesses Article 14 INC/AEV.

1.2.3–1.2.6 Vulnerability response, discovery, CVD and vulnerability management

- Vulnerability response (VR): confirm, assess, remediate, update and disclose where needed, led by PSIRT
- Vulnerability discovery (VD): internal testing, external research, scanning, user reports, supply-chain review, and similar
- Coordinated disclosure (CVD): restrict public detail until a fix is available and users have a reasonable deployment window
- Vulnerability management (VM): includes proactive testing, monitoring and supply-chain management (see VHP)

1.2.7 Product and instance

"Product" means a hardware/software unit within the CRA-applicable product list that has model and version identifiers (including support status: in sale / maintained / limited support / EOL). "Instance" means one device installed on a specific non-road vehicle or other applicable product on that list. Impact analysis is performed at the level of version plus instance reachability; see PID.

1.2.8 Incident response and vulnerability response

Incident response focuses on containing and recovering from ongoing harm. Vulnerability response focuses on planned remediation of identified weaknesses. The two may intersect: an incident may reveal a new vulnerability, or disclosure of a vulnerability may trigger an incident. When they intersect, handle and report in parallel; neither replaces the other.

1.3 Why coordinated vulnerability disclosure

1.3.1 Protect users and the safety of field operations

The primary goal of CVD is to protect end users, operators and the safety of field operations. If vulnerability details are published before the vendor completes remediation and gives users a reasonable deployment window, attackers may exploit the issue before patches are widely applied. For equipment on the CRA-applicable product list, consequences may include not only data leakage but also remote interference, control or on-site accidents. Coordinated disclosure gives the manufacturer time to remediate and roll out updates so users can obtain fixes or apply mitigations before details spread widely.

1.3.2 Build trust with the security research community

Trust between the vendor and the research community underpins effective vulnerability management. Zoomlion Product Security Incident Response (PSIRT) encourages responsible reporting through a

predictable acknowledgement and assessment process, a clear safe harbour, fair recognition and professional communication—rather than selling issues to adversaries or making uncoordinated public releases. Once trust is established, external intelligence becomes an important input to product security improvement.

1.3.3 Regulatory compliance

As cybersecurity regulation evolves worldwide, vulnerability management has moved from "good practice" to a compliance necessity. The EU CRA requires manufacturers of products with digital elements to establish vulnerability handling and reporting mechanisms. ISO/IEC 29147, 30111 and prEN 40000-1-3 PRE-2 set concrete expectations for coordinated disclosure, channel accessibility and researcher protection. This policy is the external commitment document for the PRE domain under prEN 40000-1-3.

1.3.4 Continual security improvement

The CVD process itself forms a security feedback loop: reproduction, root-cause analysis and fix verification for each valid case can reveal systemic weaknesses in design, development, supply chain or OTA processes. PSIRT periodically feeds patterns back to STRP, engineering and quality to update threat models, coding standards and test cases, enabling data-driven continual improvement.

1.4 Document overview

- Part I: Introduction
- Part II: Principles (harm minimisation, presumption of good faith, predictability, incentives, ethics, improvement, complexity)
- Part III: Parties
- Part IV: Stages (discovery → reporting → validation and rating → remediation → publication → deployment)
- Part V: Disclosure strategy, multi-party CVD, supply chain, response and confidentiality
- Part VI: PSIRT operating manual
- Annexes: report template, severity rating, disclosure request, safe harbour (including legal boundaries), FAQ, glossary, contacts, communication templates, and related materials

1.5 Policy scope

Per ENISA Coordinated Vulnerability Disclosure Policies in the EU (2022) and ISO/IEC 29147, a CVD policy must clearly define its scope so researchers can judge whether their testing and reporting fall under this policy.

Scope category	In scope	Out of scope / route elsewhere
Products	See Zoomlion CRA-applicable product list	Equipment not on the list / CRA-exempt equipment

Test environment	Owned equipment, Zoomlion written-authorised samples, isolated lab environments	In-the-field operating fleets, other parties' equipment, production OTA/cloud production (destructive/unauthorised)
Reporters	Any good-faith researcher, user or supply-chain party	Malicious exploitation, extortion, uncoordinated public disclosure of detail
Third parties	Open-source or supplier issues coordinated upstream by PSIRT	Third-party operator backbones, public DNS/CA, non-Zoomlion cloud tenants
Contractual relationship	Reporters with a product/service relationship with Zoomlion	Internal enterprise IT (non-product surface)

Public accessibility target: after security.txt (RFC 9116) goes live, the full policy or a summary, dedicated security contact details, PGP and the report form shall be published together; until then, controlled channels apply.

Part II — Principles of coordinated vulnerability disclosure

The following principles guide Zoomlion Product Security Incident Response (PSIRT) decisions in all external coordination activities and are used to assess process effectiveness.

2.1 Harm minimisation

Place end users, operators and the safety of field operations first. Use non-destructive methods for validation; ensure remediation does not introduce new defects; choose an appropriate time to publish; apply confidentiality controls throughout so that details are not disclosed prematurely to potential attackers.

- Do not perform destructive validation against in-the-field fleets, production OTA channels or other parties' equipment
- Do not test reachable instances during construction/lifting windows in ways that may affect CAN or remote control
- When publishing, provide actionable mitigations; do not provide weaponised exploitation steps

2.2 Presumption of good faith

Absent contrary evidence, treat every report as good-faith research, regardless of the reporter's identity or anonymity, and respond professionally. Those who comply with this policy are covered by the safe harbour. Maintain respectful communication even when views differ.

2.3 Process predictability

- Publish the policy, channels, acknowledgement expectations and severity definitions
- Provide timely status updates to reporters; explain reasons when timelines change
- Negotiate disclosure content and timing before publication; internal teams follow the VHP

2.4 Positive incentives

- Acknowledgement and recognition (PRE-2-RC-02), respecting anonymity
- Provide a professional, efficient handling experience

2.5 Ethics

- Research must stay within legal bounds; test only owned or written-authorised equipment/environments
- Do not access, modify or delete others' data; do not impair availability of systems in the field
- Do not use research findings for extortion, trading uncoordinated detail, or endangering personal safety
- Do not perform unauthorised remote control of production fleets or forge OTA updates

2.6 Continual improvement

- Review this policy and the public summary in full each year
- Analyse acknowledgement, remediation and disclosure metrics quarterly (with the VHP)
- Extract design-defect patterns from each valid case and feed them back to STRP/engineering

2.7 Inherent complexity

CVD is a complex problem: unclear boundaries, conflicting multi-party goals, and no single perfect answer. Each case needs situational judgement; flexible adaptation and multi-party cooperation take priority over pursuing a “perfect process”.

2.8 Mutual obligations (ENISA / BSI / CCB practice)

A CVD policy should state mutual obligations of the vendor and the reporter. Following German BSI guidance, researchers are not required to sign a formal contract, MoU or NDA when reporting a vulnerability. This policy itself constitutes the testing authorisation and safe-harbour boundary statement, subject to the ground rules.

2.8.1 Vendor (Zoomlion / PSIRT) obligations

- Receive, acknowledge and handle valid reports in good faith and in a timely manner; provide predictable communication
- While the reporter complies with this policy, do not initiate civil or criminal proceedings (safe harbour; boundaries in Annexes C and G)
- Keep report content confidential; do not disclose the reporter's identity to third parties without consent (except anonymous reports)
- Remediate or mitigate within a reasonable and flexible timeframe
- Provide a dedicated security contact channel: vsoc_wlaq@zoomlion.com
- Offer acknowledgement or rewards for valid contributions

2.8.2 Reporter obligations

- Observe proportionality: limit testing to the minimum access and data strictly necessary to demonstrate the vulnerability
- Do not conduct DDoS, social engineering, brute-force attacks, malware installation, persistent privilege maintenance or password theft
- Do not intentionally intercept, record or access non-public communications; do not modify or delete data beyond the authorised scope
- Report promptly through official channels after discovery; do not share details with third parties before coordinated disclosure is complete
- Reports must include a clear description, reproduction steps, tools used, discovery time, impact and a non-weaponised PoC
- Personal/customer data encountered: retain the minimum necessary, do not redistribute, delete after demonstration and inform PSIRT
- Where cross-border or export-control sensitive content is involved, cooperate with PSIRT legal assessment of the transfer scope

Part III — Parties to coordinated vulnerability disclosure

3.1 Finder

The individual or organisation that first identifies the weakness. A finder is not automatically the reporter. Zoomlion encourages finders to become reporters by using PSIRT official channels.

3.2 Reporter

- Submit via official channels; provide reproducible information; cooperate with confirmation
- Keep confidentiality until written permission is granted or the agreed period ends
- Do not exploit the vulnerability maliciously

3.3 Product vendor (manufacturer)

The vendor role is performed by Zoomlion Heavy Industry Science & Technology Co., Ltd. The operating body is Zoomlion Product Security Incident Response (PSIRT). Responsibilities include receiving reports, distributing them for validation and remediation to the relevant units, coordinating disclosure, and providing update guidance to affected users.

3.4 Product users

Vehicle OEMs, lessors/owners, sales and service organisations, and operators. Duties: follow advisories, deploy updates in the security window, apply mitigations when immediate update is not possible, and report update issues.

3.5 Coordinating body

A neutral facilitator (national CSIRT, CERT, vulnerability platform, etc.) used for multi-vendor cases, trust gaps, large-scale notification or anonymous mediation. By default, Zoomlion Product Security Incident Response (PSIRT) is the manufacturer-side central coordination point.

3.6 Other stakeholders

- Module/chip suppliers, cloud platform operators, and similar parties
- Overseas agents (user notification within authorised scope)
- Regulators (Article 14 SRP and similar)

Part IV — Stages of the coordinated vulnerability disclosure process

4.1 Discovery stage

Good-faith research is welcome. Researchers should minimise risk: use isolated environments, owned or authorised equipment, back up before testing, stop immediately if a mass-exploitable issue is found to avoid excessive access, and keep research logs. Do not attempt exploitation that may affect the safety of construction machinery operating in the field.

4.2 Reporting stage

Channels must be available, secure, traceable and responsive. All channels enter the same VTI and SLA; priority is not reduced because of disability, language or assistive technology.

Channel	Address / location	Ack target	Notes
Security mailbox (PGP recommended)	vsoc_wlaq@zoomlion.com	2 working days	See SCOM; suitable for detailed technical reports
Phone / voice assistance	+86 4008000157	Business hours; operator records and reads back	PRE-2 multi-sensory; not the sole channel

4.2.1 Accessibility and multi-sensory access (PRE-2-RC-01)

Two sensory channels: the electronic channel supports keyboard and screen readers; the voice channel is transcribed by an operator using standard fields and read back for confirmation.

Recommended report content

- Product model, hardware and software/firmware versions, configuration environment
- Vulnerability type and attack vector (cellular / OTA / CAN / local diagnostics / cloud interface, etc.)
- Reproduction steps, non-weaponised PoC, impact and attack prerequisites
- Evidence (logs/screenshots; avoid real user data)
- Discovery date, whether already public, and contact details (anonymity optional)

4.3 Validation and rating stage

- Completeness check, scope confirmation, duplicate check, isolated reproduction, impact confirmation

- After a complete report: initial assessment within 3 working days for Critical/High; 7–14 working days for others (internal P0 still follows the VHP)
- If information is incomplete, request clarification; after up to three rounds the case may be closed with an explanation
- Inform the reporter whether the report is accepted, the initial severity and the expected timeline

4.3.1 PSIRT final assessment authority

Zoomlion Product Security Incident Response (PSIRT) retains final decision authority on report validity, severity, remediation timeline, and disclosure timing and content. Reasons are communicated transparently and dialogue is maintained, but the decision is internally binding. If disclosure agreement with the reporter cannot be reached, protection of users and operational safety takes highest priority.

4.3.2 Out-of-scope vulnerability types

The following types normally do not enter acknowledgement assessment; they may still be recorded as intelligence at PSIRT's discretion. Clearly malicious cases are escalated to legal:

- Zoomlion products outside the declared support scope
- Pure social engineering, physical vehicle theft, or destructive teardown without evidence of a product design defect
- DoS against third-party cellular-operator backbones or public Internet infrastructure
- Non-product issues that exist only on marketing websites/documentation (routed to the relevant team; not under product CVD SLA)
- Scanner output, theoretical issues or informational descriptions without reproducible evidence or exploitability
- Laboratory conditions requiring destructive hardware attacks that do not match a reasonable attacker model (unless mass-production reproducibility is shown)
- Weak-password guessing / rate-limiting issues without demonstrated authentication bypass
- Scenarios that require the tester to interfere with the safe operation of in-the-field equipment on a worksite

4.4 Remediation stage

Remediation should address the root cause and be secure, stable, as compatible as practicable, and verifiable. Internally, execute VHP RMD. Provide mitigations when a patch cannot be released immediately. External timeline commitments apply.

4.5 Public disclosure stage

After a fix is available and users have a reasonable deployment window, publication helps unpatched users protect themselves, supports community learning and regulatory transparency. Advisory drafts may be shared with the reporter for comment (without spreading unpublished exploit detail).

- Advisory ID ZL-SA-YYYY-NNN, date, affected products and versions, overview (no weaponised steps), severity, fixed version and guidance, CVE/EUVD (if any), acknowledgement, reference links
- Publication channels: vsoc_wlaq@zoomlion.com, authorised website/agents, CVE/NVD/EUVD synchronisation

4.5.2 Coordinated public disclosure (synchronisation principle)

Any public disclosure shall be synchronised with the reporter and any involved upstream parties. In principle, publish together: a vulnerability overview (without weaponised steps), affected versions, and remediation/mitigation with how to obtain them. If the issue affects third-party components or similar stacks used by other organisations, notify those parties directly before publication. User notification means include ZL-SA, mailing lists and OTA push (DIST/PRA).

4.5.3 Coordinating body and upstream non-response

- Researchers may report to PSIRT first; the manufacturer coordinates upstream so researchers need not face cross-border legal risk alone
- If an upstream component vendor does not respond for a prolonged period: PSIRT applies compensating controls, extends the coordination window and explains the dependency transparently to the reporter
- Where appropriate, engage a national CERT/CSIRT as a neutral coordinator (with reporter consent and after assessment)
- If the manufacturer does not respond to the reporter, researchers may contact their Member State CERT

4.6 Fix deployment and promotion stage

On the CVD side, PSIRT coordinates with the reporter on when users can obtain the fix. Deployment-rate targets are defined in VHP PRA.

Part V — Process variations and practical guidance

5.1 Disclosure strategy selection

- Default: coordinated disclosure; default non-disclosure period is 90 days and may be extended in writing
- In-the-wild exploitation or Article 14: protective notification may come first; technical detail remains controlled
- Refuse full publication of exploit detail where doing so would significantly increase in-the-wild exploitation risk

5.2 Bilateral and multi-party CVD

Bilateral: reporter ↔ PSIRT. Multi-party: when module vendors, crypto chips, cloud platforms or similar are involved, coordinate under TR 5895; Zoomlion keeps the manufacturer master record and may involve a CERT where needed.

5.3 Complex supply chains

When upstream parties do not respond within the timeline, apply VHP complexity extensions and compensating controls. Do not conceal from the reporter that the root cause is upstream, but third-party confidential detail may be limited.

5.4 Response times and disagreements

Conference or planned public-disclosure needs should be raised early. Dispute handling: prioritise protection of users and operational safety; seek an acceptable compromise; if agreement cannot be reached, PSIRT may publish limited information after the agreed period under this policy. Communication is managed centrally by the coordinator to avoid conflicting messages.

5.5 Confidentiality before disclosure

- Vulnerability information is stored in controlled systems with TLP/internal classification marking
- External sharing only via SCOM

Part VI — Zbox PSIRT operating manual

This section corresponds to industry “product security incident response / PSIRT” operating functions. Within Zoomlion it is performed by Central Research Institute PSIRT; no external brand name is established or cited.

6.1 Internal workflow

- Intake → assign ZL-VULN-YYYY-NNN → acknowledge within 24 hours / 2 working days
- Triage: scope / duplicate / P0 flag → isolated reproduction → rating → handling plan
- Iterate fixes with engineering/OTA → verify → advisory and distribution → PRA
- If Article 14 is triggered, run statutory reporting timelines in parallel; CVD negotiation shall not delay SRP or protective notification

6.2 Roles and responsibilities

- PSIRT lead: policy, resources, major cases, external messaging, assignment to executing units
- Coordinator: reporter communication, disclosure negotiation, acknowledgement/reward process
- Product security engineer (executing unit): reproduction and rating
- Engineering interface: remediation and updates
- Legal: safe harbour and sensitive information

6.4 Escalation

Level	Trigger	Escalation path
Level 1	Ack SLA breach; repeated incomplete information	Coordinator → vulnerability management engineer
Level 2	Critical; indicators of in-the-wild exploitation	Product security → PSIRT lead
Level 3	Article 14; personal/vehicle operational safety; media	PSIRT lead → management / legal

6.5 Violations, exceptions and approval

- Researchers who breach ethics or the safe-harbour boundary: stop the CVD process and refer to legal assessment; the case may still be recorded as intelligence without a reward/acknowledgement commitment
- Internal staff who breach OPSEC or make unauthorised external disclosure: handle under company discipline and information-security rules, and trigger leak response (see OPSEC §8.2)
- Shortening the non-disclosure period or publishing exploit detail early: requires written approval by the PSIRT lead and Legal, with rationale and user-risk trade-off recorded
- Reward exceptions (e.g. early partial incentive for Critical, if a programme exists): joint approval by the PSIRT lead and Finance/Legal
- All exceptions are linked to the VTI and retained for ≥ 10 years; approval form ID: CVD-EXC-001

6.5.1 Violation categories (examples)

Category	Examples	Immediate action
Process	Ack SLA breach without escalation; unencrypted PoC sharing; conflicting external messaging	Correct + COM record + escalate per OPSEC
Confidentiality	Leak of detail during the non-disclosure period; unauthorised media comment	Legal + leak emergency (OPSEC §9.4)
Research boundary	Testing in-the-field vehicles; unauthorised data access; extortion	Stop safe-harbour reliance; escalate to legal
Disclosure	Publishing exploit detail before release gates; ZL-SA conflicts with Article 14 messaging	Correction/withdrawal assessment + notify management

6.5.2 Exception approval

Exception type	Approver	Minimum attachments	Maximum validity
SLA extension (not Article 14 / in-the-wild)	PSIRT lead; high complexity + management informed	Compensating controls, user mitigations, re-review date	As stated in writing
Non-disclosure period extension	PSIRT lead + legal	Reporter negotiation minutes; fix/deployment status	Single extension ≤ 30 days; cumulative rationale in VTI
Limited protective notice (before fix)	PSIRT lead + legal; Article 14 in parallel	Draft without exploit detail; notification channel list	Event-driven
Waive a coordinated-disclosure control point (rare)	PSIRT lead + legal + management	Risk acceptance; alternative controls; user impact assessment	Single case

All exceptions must be written into the VTI master record with an exception reference. Oral approval is allowed only for P0 emergencies and must be documented in writing within 24 hours. Article 14 / in-the-wild scenarios shall not use a routine SLA extension as a reason to omit notification or reporting.

Supporting indicators: P0 4-hour judgement rate, overdue non-disclosure periods without disclosure, Article 14 window compliance, Critical deployment rate. Share data sources with VHP §9 to avoid metric drift.

Annex A — Vulnerability report template

Suggested subject: `[Zoomlion CVD] <one-line vulnerability title> — <model/version>`

Field	Guidance
Contact	Name/alias or anonymous; email; PGP fingerprint (optional)
Product	Model; HW/SW versions
Environment	Lab / authorised sample; whether connected to enterprise platform
Vulnerability type	e.g. RCE, auth bypass, firmware signature verification, OTA, clear-text sensitive data
Attack prerequisites	Network, privileges, physical proximity, user interaction
Reproduction steps	Numbered steps allowing PSIRT to reproduce independently
Tools used	Scanner/debug/framework name and version (if applicable)
Discovery time	First discovery date (approximate is acceptable)
PoC	Non-weaponised; no real customer data
Impact	C/I/A and any operational-safety impact
Already public?	Yes / No / link
Disclosure plan	Whether conference publication is intended; preferred timing

Annex B — Vulnerability severity rating guide

B.1 Severity definitions

Level	Definition summary	External remediation expectation
Critical	Remote control / severe security or privacy impact and easy to exploit; or affects operational safety	Priority emergency path; take the stricter of this policy and VHP
High	Significant C/I/A impact or exploitation with few prerequisites	≤ 90 working days external commitment cap
Medium	Exploitable under limited conditions	≤ 90 working days cap
Low	Very small impact or extremely hard to exploit	≤ 180 working days

B.2 CVSS v3.1 and operational-safety weighting

CVSS provides the base score. Where remote vehicle control, OTA integrity, CAN-related commands or personal safety at the worksite are involved, PSIRT may raise severity and trigger VHP P0/P1 processes.

Weighting factor	Description	Possible action
Operational safety	May cause unintended motion, loss of control or personal risk	Raise severity; assess Article 14
In-the-wild exploitability	Public exploit exists or attacks observed	Shorten disclosure negotiation; protective notification
Attack-surface reachability	Network-reachable vs physical diagnostics required	Affects AV/AC and priority
Data sensitivity	Includes location / operating condition / key material	Privacy and notification assessment

Annex C — Safe harbour terms

Authorised scope

- Good-faith security research against Zoomlion products and supporting components within the declared support scope
- Use of owned equipment/environments or those authorised in writing by Zoomlion
- Prompt reporting through official channels and confidentiality before remediation

Authorised testing boundaries

- Do not access unauthorised data or other parties' instances
- Do not perform destructive tests against production/in-the-field vehicles or cloud production environments
- Do not perform operations that could endanger personal safety or construction-machinery operational safety
- Do not extort, trade uncoordinated detail, or publicly release “0-days”

Legal commitment

For good-faith research that complies with this policy, Zoomlion Heavy Industry Science & Technology Co., Ltd. will not initiate civil litigation or criminal complaints. This commitment is not a complete waiver under every jurisdiction.

Exclusions

- Using a security vulnerability to commit crimes, extortion, or intentional harm to persons or property
- Conduct that bypasses the prohibitions expressly stated in this policy
- Attacks against unauthorised third-party systems or operator infrastructure
- Conduct that violates export control, data protection or applicable labour law

Annex D — Frequently asked questions (FAQ)

Q: Who may report?

A: Anyone. Even if you are not a professional researcher, you may report abnormal security behaviour; more complete technical detail is better.

Q: May I remain anonymous?

A: Yes. Leaving a contact email is recommended for acknowledgement and status updates; PGP may be used. Anonymity may affect acknowledgement and reward payment.

Q: How long for acknowledgement?

A: Email: 2–5 working days. If you receive nothing, check spam and contact via a second channel.

Q: When may I publish?

A: Coordinated disclosure is the default. You need written permission, or the non-disclosure period to have expired with PSIRT notified. Do not publish exploit detail before a fix.

Q: What if it is a third-party component vulnerability?

A: Report to PSIRT first. The manufacturer coordinates upstream unless PSIRT expressly instructs parallel notification to the upstream vendor.

Q: May I test company equipment?

A: Only owned or written-authorised samples. The safe harbour does not authorise testing other parties' equipment or vehicles operating in the field.

Q: How do I obtain an SBOM?

A: After assessment, you may request from PSIRT permission to obtain component information relevant to security research.

Q: Is there a bounty?

A: Whether or not a bounty exists, valid reports are handled under this policy and acknowledged (with consent).

Q: What if this conflicts with Article 14?

A: Statutory protective notification and SRP take priority; that does not mean full exploit detail will be published.

Q: The channel is not on the website yet?

A: Until addresses are confirmed, submit via the temporary interface Zoomlion has designated in writing; after confirmation, follow the security page.

Q: May I report EOL versions?

A: Yes. Remediation commitments depend on support status. EOL products may receive only mitigations or an upgrade recommendation, which will be stated after acknowledgement.

Q: What if I find multiple vulnerabilities?

A: Report each root-cause class separately for tracking where possible; if they form one root-cause chain, link sub-items under one VTI.

Q: Conference/CTF disclosure?

A: State the planned disclosure date and venue as early as possible; PSIRT will assess whether accelerated remediation or written permission is needed.

Q: Can I obtain test equipment?

A: Mass-production in-the-field equipment is not provided. After assessment, authorised samples or isolated-environment guidance may be offered.

Q: The vulnerability is already public but I just found it?

A: Still report it and include the public link and timing; already-public cases follow an accelerated assessment and notification path.

Annex E — Glossary

Term	Description
PSIRT	Zoomlion Product Security Incident Response Team performing SRC/PSIRT functions
VTI	ZL-VULN-YYYY-NNN
ZL-SA	Security advisory ID ZL-SA-YYYY-NNN
Non-disclosure period	Agreed period during which technical details shall not be published
Safe harbour	Boundary of the commitment not to initiate legal action against good-faith research under this policy
NDP / non-disclosure period	Non-Disclosure Period; no publication of technical detail within the coordinated disclosure window
SFOP	Safety Field Operational Priority; worksite operational-safety priority weighting
ITW	In-The-Wild; indicators of exploitation in the field
COM	Communication record requirements in ZL-SEC-COM-001
RCE	Remote Code Execution
PoC	Proof of Concept; must be non-weaponised

Annex F — Communication template library

The following templates are for coordinators to send via SCOM. Replace angle-bracket placeholders, link the VTI and record in COM. English versions are for cross-border reporters.

F.1 Reporter acknowledgement template

English

Subject: [Zoomlion CVD] We have received your report — VTI: <ZL-VULN-YYYY-NNN>

Hello,

Thank you for submitting a security report to Zoomlion PSIRT. We have assigned tracking ID <ZL-VULN-YYYY-NNN> and expect to complete an initial assessment and contact you again by <date / working day>.

Please do not publish technical details or a PoC until coordinated disclosure is complete. If we need more material, we will contact you on this channel.

Confidentiality: do not share sensitive detail in clear-text instant messaging.

This message confirms receipt only and is not a determination that a vulnerability exists or of its severity.

Zoomlion PSIRT
vsoc_wlaq@zoomlion.com

F.2 Clarification request template

Subject: [Zoomlion CVD] Request for additional information — VTI: <ZL-VULN-YYYY-NNN>

Hello,

Regarding VTI <ZL-VULN-YYYY-NNN>, to reproduce and assess in an isolated environment, please provide:
1) affected product model and HW/SW versions; 2) reproduction steps; 3) attack prerequisites and environment; 4) (if applicable) a non-weaponised PoC or log excerpt (please encrypt attachments).

If we do not receive a reply by <date>, we may place the case on hold and explain why; you may resubmit complete information at any time.

Zoomlion PSIRT

vsoc_wlaq@zoomlion.com

F.3 Rejection / out-of-scope template

Subject: [Zoomlion CVD] Scope notice — VTI: <ZL-VULN-YYYY-NNN>

Hello,

Thank you for your submission. After initial assessment, this report is outside the current CVD policy scope for the following reason: <brief explanation>. We will therefore not continue tracking under the product CVD SLA.

If you believe the scope decision is incorrect, please provide additional model, version and reproduction material.

Thank you for your interest in Zoomlion product security.

Zoomlion PSIRT

vsoc_wlaq@zoomlion.com

F.4 Disclosure negotiation template

Subject: [Zoomlion CVD] Coordinated disclosure negotiation — VTI: <ZL-VULN-YYYY-NNN>

Hello,

A fix/mitigation is <available / planned>. We propose a coordinated disclosure window of <date>; planned ZL-SA summary: <overview without weaponised steps>.

Please confirm timing, acknowledgement preference and intended public scope. Full exploit detail requires a patch to be available with a reasonable user deployment window, or written PSIRT permission.

Zoomlion PSIRT

vsoc_wlaq@zoomlion.com

F.5 Status update template (periodic communication)

Subject: [Zoomlion CVD] Status update — VTI: <ZL-VULN-YYYY-NNN>

Hello,

VTI <ZL-VULN-YYYY-NNN> current status: <Under review / Fix in progress>. Next step: <planned action>; next update expected: <date>.

This message does not contain exploit detail. Please reply on this channel if you have questions.

Zoomlion PSIRT

F.6 Case closure notice template

Subject: [Zoomlion CVD] Case closed — VTI: <ZL-VULN-YYYY-NNN>

Hello,

VTI <ZL-VULN-YYYY-NNN> is closed. Fix/advisory: <ZL-SA link or summary>. Acknowledgement: <listed / anonymous / not applicable>.

Thank you for reporting responsibly. You are welcome to submit new issues through the official channels.

Zoomlion PSIRT

vsoc_wlaq@zoomlion.com

Annex G — Legal and compliance boundaries

G.1 Not covered by the safe harbour

- Intentionally endangering personal safety, damaging in-the-field operational equipment, or extorting users
- Unauthorised access to, download of, or retention of others' data beyond the minimum needed to demonstrate the vulnerability
- Research that violates applicable export controls, data protection laws, sanctions lists or cross-border data-transfer restrictions
- Monetising vulnerabilities, selling 0-days, or leaking uncoordinated detail to media or criminal markets
- Impersonating Zoomlion staff, forging acknowledgements, or phishing other researchers
- Other exclusions listed in Annex C

G.2 Data protection and privacy

- Reports must not include real customer names, precise geographic tracks, licence plates/VIN or similar identifiers; use redacted or laboratory data
- Personal data received by PSIRT is handled on a minimum-necessary basis with restricted access; retention follows the VHP/company rules
- Cross-border transfer of research material uses SCOM-approved channels;
- Anonymous reports may still constitute personal data (IP/email);

G.3 Legal-risk notice for researchers

ENISA notes that researchers in the EU often face uncertainty under criminal law, copyright, data protection, contract and export control. This policy's safe harbour aims to reduce risk for good-faith reporting under the policy within applicable law, but is not an exemption for every jurisdiction or every act. Cross-border reporters should assess local law themselves; Zoomlion will provide guidance under the law of the manufacturer's jurisdiction and target markets.

Legal domain	Typical risk	Mitigation under this policy
Criminal / unauthorised access	Scanning/testing may engage computer-crime provisions	Explicit authorisation boundary in the policy + safe harbour (Annex C)
Copyright / anti-circumvention	Reproduction involves firmware/code fragments	Minimum material for validation only; legal review of sensitive sharing
Data protection (GDPR/PIPL etc.)	Incidental personal data	Minimum necessary, deletion, access restriction

Contract / EULA	Reverse-engineering prohibitions	Policy authorisation prevails over general marketing EULA research exceptions as stated
Export control	Cross-border crypto/technical data	SCOM/legal approved channel