HITACHI

Hitachi Rail

Coordinated Vulnerability Disclosure Policy

We do not give or accept business courtesies to influence business decisions. We fulfil the requirements of this Procedure and similarly respect the policies and procedures of those with whom we exchange business courtesies.

Application & Classification	Effective Date	Document Reference Codes
Hitachi Rail - Global Hitachi Rail - Internal	10 September 2026 or at a later date if any notification or consultation is required under local law or regulation	

Document Identifier Radical	DTC	Enterprise Identifier	Revision

Legacy, Consortium or Customer secondary Identifier + revision [N/A]

Contents

Document Identifier Radical	DTC	Enterprise Identifier	Revision

Legacy, Consortium or Customer secondary Identifier + revision [N/A]

01. Introduction

Cybersecurity is a key priority for Hitachi Rail. We believe that the proper and timely handling software vulnerabilities is a critical factor in reducing cybersecurity risks to our customers. We are committed to coordinating directly with security researchers, customers, and other stakeholders from initial vulnerability reporting through final resolution and responsible disclosure.

Our formal vulnerability handling and disclosure guidelines outline a swift, risk-first response. By prioritising known exploits alongside critical and high-severity issues, Hitachi Rail ensures significant threats are resolved rapidly and effectively.

1.1. Purpose

A vulnerability is a weakness that could compromise the confidentiality, integrity, or availability of a product, service, component, or system.

This Vulnerability Disclosure Policy establishes the framework for responsible reporting, assessment, remediation, and disclosure of cybersecurity vulnerabilities affecting Hitachi Rail products and services.

Hitachi Rail maintains vulnerability handling processes throughout the supported lifecycle of Products with Digital Elements and makes security updates available in accordance with applicable regulatory obligations and product support commitments.

This Policy aligns with ISO/IEC 29147 for vulnerability disclosure, ISO/IEC 30111 for vulnerability handling processes, and applicable legal, regulatory, and contractual requirements.

1.2. Scope

This Policy applies to vulnerabilities affecting products with digital elements developed, maintained, supported, or supplied by Hitachi Rail, whether identified internally or reported by customers, security researchers, suppliers, or other third parties. Hitachi Rail also evaluates vulnerabilities originating from third-party components, open-source software, libraries, and supplier-provided technologies incorporated into supported products.

Even though customer-specific security configuration issues or compromised credentials are not considered a Hitachi Rail vulnerability, Hitachi Rail encourages any such findings to be reported as well.

Furthermore, Hitachi Rail, at its sole discretion, will determine if end-of-life or unsupported products are covered by this policy.

02. Product Security Incident Response Team

Hitachi Rail has established a Product Security Incident Response Team (PSIRT) responsible for coordinating vulnerability handling activities across the organisation.

The PSIRT acts as the primary point of contact for vulnerability reports and coordinates investigations with engineering, development, product management, customer support, legal and compliance functions. It also oversees communications with vulnerability reporters, customers, suppliers, and relevant coordination bodies throughout the vulnerability lifecycle.

Based on ISO/IEC 29147, ISO/IEC 30111 and the FIRST.org framework for PSIRT services, Hitachi Rail organises its CVD process into four main stages: reception of vulnerability report, validation and triage, remediation, and disclosure to customers and authorities.

03. Coordinated Vulnerability Disclosure

Hitachi Rail supports Coordinated Vulnerability Disclosure as the preferred approach for managing cybersecurity vulnerabilities. Hitachi Rail collaborates with customers, security researchers, suppliers, and other stakeholders to reduce cybersecurity risks and implement appropriate corrective actions.

Under this approach, vulnerability information is shared with Hitachi Rail in a responsible manner, allowing sufficient time for investigation, validation, risk assessment and the development of mitigations or corrective actions before public disclosure occurs.

Hitachi Rail believes that coordinated disclosure provides the greatest benefit to customers and users by reducing the possibility that vulnerability information may be exploited before protective measures become available.

3.1. Good-Faith Research and Safe Harbor

Hitachi Rail supports legitimate security research conducted in good faith.

Researchers avoiding privacy violations, service disruption, safety impacts and unauthorised disclosure of information, will not be subject to legal action by Hitachi Rail for activities conducted in compliance with this Policy.

Activities that could affect railway operations, safety-critical systems, customer data or service availability are not authorised unless explicitly approved by Hitachi Rail.

This commitment does not extend to activities that violate applicable laws or regulations, result in unauthorised access to data, or intentionally disrupt systems, services or operations.

3.2. Reporting a Vulnerability

Individuals or organisations who become aware of a potential cybersecurity vulnerability affecting a Hitachi Rail product or service are encouraged to report it as soon as possible. To help protect customers and users, reporters are requested to maintain confidentiality and refrain from publicly disclosing vulnerability information until appropriate mitigations or corrective actions have been made available.

Reports should be submitted to the Hitachi Rail PSIRT through the designated security contact channel: cert@hitachirail.com

Reporter is encouraged to encrypt sensitive information attached to email using Hitachi Rail CERT Public PGP Key.

PGP Key fingerprint: 8BF84AE9168CE2C3BD9C2B4BC0071E1A1198A103

To facilitate assessment and validation, reporters should provide where available:

- the affected product and version
- a description of the issue
- reproduction steps
- proof-of-concept material
- the potential impact
- contact details for follow-up communications

The reporter’s personal data is only used for actions related to the reported security vulnerabilities. It will not be disclosed to third parties without the reporter's permission, unless required by law.

3.2.1. Communication with Vulnerability Reporters

Hitachi Rail values the contribution of security researchers and is committed to maintaining an open, professional, and collaborative dialogue throughout the vulnerability handling process.

Upon receipt of a vulnerability report, the PSIRT will acknowledge the submission (typically within 7 days) and, where appropriate, provide a tracking reference. During the assessment and remediation phases, Hitachi Rail may contact the reporter to request additional technical information, clarify reported findings, or discuss potential impacts.

We will inform the reporter of the verification status and the next steps. The verification confirmation timeline will be created during the first email exchanges.

Hitachi Rail will make reasonable efforts to provide status updates during the investigation process while protecting sensitive information and respecting confidentiality requirements.

Where a vulnerability is confirmed, Hitachi Rail will seek to coordinate disclosure activities with the reporter and, when appropriate, discuss anticipated remediation and publication timelines.

Subject to the reporter's consent, Hitachi Rail may publicly acknowledge the contribution of the researcher in a related Cyber Security Advisory or security communication.

3.3. Validation and Triage

All vulnerability reports are reviewed through a PSIRT-managed process. Hitachi Rail assesses the completeness and validity of each report, reproduces the reported vulnerability where feasible, identifies affected products and their support status. Once vulnerability is confirmed, PSIRT performs triage activity evaluating severity, exploitability, and potential business impact using the Common Vulnerability Scoring System (CVSS) and the relevant product context of use / deployment.

The outcome of the assessment and validation activities is communicated to the reporter. Communication will include timeline and next steps.

3.4. Remediation

Validated vulnerabilities are managed in coordination with relevant development, engineering, product, and operational teams. Hitachi Rail performs root-cause analysis and defines appropriate corrective actions, mitigations, or security updates. Remediation priorities and timelines are determined based on factors such as severity, exploitability, affected products, operational impact, and lifecycle status.

The vulnerability management process includes intake and registration, triage and severity classification, technical validation, remediation planning and implementation, coordinated communications, security advisory publication where appropriate, and formal closure of the vulnerability record.

3.5. Disclosure

Hitachi Rail follows the principle that vulnerability information should be disclosed responsibly and, whenever possible, only after remediation measures or risk-reducing mitigations have been developed

When appropriate, Hitachi Rail may publish Cyber Security Advisories to communicate information regarding affected products, potential impacts, available mitigations and corrective actions. Customers may additionally be informed through contractual support channels, security mailing lists, or other established communication mechanisms.

The Cyber Security Advisory includes vulnerability identifiers, affected products and versions, severity information, mitigation guidance and remediation details. Where agreed, advisories may also acknowledge the contribution of the reporting researcher.

Vulnerability information will be treated confidentially and shared strictly on a need-to-know basis until an agreed disclosure strategy has been implemented.

Hitachi Rail may coordinate disclosure timelines with the reporter but reserves the right to determine final disclosure dates based on customer protection, operational safety, and regulatory requirements.

04. Regulatory and Legal Requirements

Where required by applicable laws and regulations, vulnerabilities and related cybersecurity incidents may be subject to regulatory reporting requirements. In those cases, Hitachi Rail will cooperate with competent authorities, CSIRTs and relevant regulatory bodies. Such activities are managed through dedicated internal governance and compliance processes.

Personal data submitted as part of a vulnerability report will be processed in accordance with applicable data protection legislation and Hitachi Rail privacy requirements.

Hitachi Rail
www.hitachi.com