ReeR Security Vulnerability Handling Process

1. REER'S COMMITMENT TO SECURITY

ReeR takes product security seriously and encourages responsible disclosure of vulnerabilities. This document outlines the steps followed by the ReeR PSIRT team to evaluate and handle reported vulnerabilities, including the criteria for publishing security advisories.

2. VULNERABILITY HANDLING PROCESS

All reported vulnerabilities are processed through the following phases:

- Phase 1 - Report Submission:

Vulnerabilities should be reported to the ReeR PSIRT team via email at psirt@reer.it. Reports should include a clear problem description, technical details, potential impact, and reproduction steps if available. Acknowledgment of receipt will be sent within two business days.

- Phase 2 - Analysis and Verification:

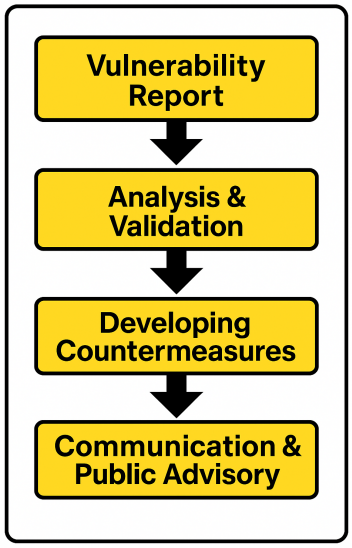
The PSIRT team reviews the report to verify its authenticity, relevance, and impact on ReeR products. We may request additional technical details if needed.

- Phase 3 - Mitigation Development:

Verified vulnerabilities are escalated to the responsible development teams. Fixes or temporary mitigations are developed and may be shared with the reporter for validation.

- Phase 4 - Public Disclosure:

Once fixes are validated, ReeR issues a public advisory that includes technical details, affected products, impact, mitigation or resolution steps, and reporter credit if desired.



3. RESPONSIBLE DISCLOSURE POLICY

ReeR supports coordinated vulnerability disclosure. We work with reporters to ensure proper fixes are available prior to public disclosure. Advisories are published on ReeR's official site and contain necessary risk mitigation details.

4. STRUCTURE OF REER SECURITY ADVISORIES

Each advisory follows a consistent structure:

- Title: Descriptive name summarizing the vulnerability and product.
- Advisory ID: Unique reference number.
- Revision History: Log of changes to the advisory.
- Description: Technical overview of the issue.
- Affected Products: List of impacted ReeR products.
- Impact: Description of the potential outcome if exploited.
- Classification: CVSS v3 score and vector.
- Temporary Mitigations: Workarounds to reduce risk.
- Remediation: Fixes or patches issued.
- References and Legal Notice
- Acknowledgements: Optional credit to the reporter.

5. CONTACT INFORMATION

For any inquiries regarding this process or to report a vulnerability, contact us at:

Email: psirt@reer.it