Open Regulatory Compliance

Comments on CEN/CENELEC PT3 Vulnerability Handling Standard

2.9 | Inputs & contributions

Deliverable:	2.9
Category:	Inputs & contributions
Owner:	Cyber Resilience SIG
Status:	Shipped
License:	CC-BY-SA 4.0
Date:	December 2025

SIG: Cyber Resilience SIG
Document type: Deliverable
Number: 2.9
Status: Submitted
Group: CEN/CENELEC WG 9
Subgroup: PT 3
Date: 2025-08-04

Feedback to CEN/CENELEC PT3 Vulnerability Handling

The current use of ISO/IEC 29147 in the PT3 draft appears incompatible with the Cyber Resilience Act (CRA) when applied to open source software. The CRA introduces a more nuanced understanding of software supply chains, particularly with respect to the role of open source, which is not adequately reflected in ISO/IEC 29147 or ISO/IEC 30111. We respectfully submit the following concerns and recommendations:

1. Misalignment in actor definitions

- The CRA clearly distinguishes between manufacturers, users, open source projects, and, where applicable, open source stewards. However, the PT3 draft interprets vendor as equivalent to manufacturer, and further assumes that open source projects can be treated as vendors.
- This chain of equivalencies manufacturer = vendor = open source project fails to capture the functional and legal distinctions between these actors and ultimately omits a crucial class of stakeholder: the open source steward.
- Moreover, ISO/IEC 29147 defines vulnerability coordination solely among four actors: users, vendors, reporters, and coordinators. There is no recognition of open source projects or stewards as distinct roles with unique constraints, governance models, and obligations.

2. Inadequate treatment of open source in the standard

• Open source is not a vendor: The current definition of manufacturer in the PT3 draft does not adequately account for open source projects. A new term such as vendor has been proposed, but it remains ambiguous and insufficient. Open source projectsespecially community-driven onesdo not have legal or commercial obligations equivalent to those of manufacturers. Their inclusion as vendors risks inappropriate liability expectations and misunderstanding of open source governance.

• Stakeholder inclusion: The list of stakeholders must be expanded to explicitly include both open source stewards and open source projects without stewards. These actors operate differently from traditional manufacturers and require differentiated treatment in processes related to vulnerability handling and compliance.

3. Vulnerability handling and responsibilities

• Open source project expectations: It is inappropriate and unrealistic to expect open source projects to directly handle vulnerability disclosure requests in the same manner as vendors. Manufacturers (or product integrators) should be responsible for evaluating and responding to vulnerabilities in the open source components they use, particularly when they modify or redistribute them.

• Comprehensive vulnerability sources: The list of acceptable sources of vulnerability reports should be expanded to include dedicated channels established by manufacturers themselves. This ensures they can receive and process vulnerabilities related to their implementation of open source components.

• Remediation strategies: The standard should acknowledge that a common remediation approach for vulnerabilities in open source components is the application of patches or updates provided by the upstream project. This practice reflects the decentralized and collaborative nature of open source maintenance.
4. Versioning and transparency

• Open source versioning in SBOMs: For open source components, versioning is inherently complex due to the potential for manufacturer-level modifications or forks. Therefore, the SBOM must explicitly declare any patches or changes applied to upstream open source software to maintain transparency and enable accurate vulnerability assessments.

• Machine-readable SBOMs: The requirement for machine-readable SBOMs should be stated directly within the normative core of the standard, not merely in the acceptance criteria. This is essential to support automated analysis, tooling interoperability, and the efficiency of vulnerability management workflows across supply chains.