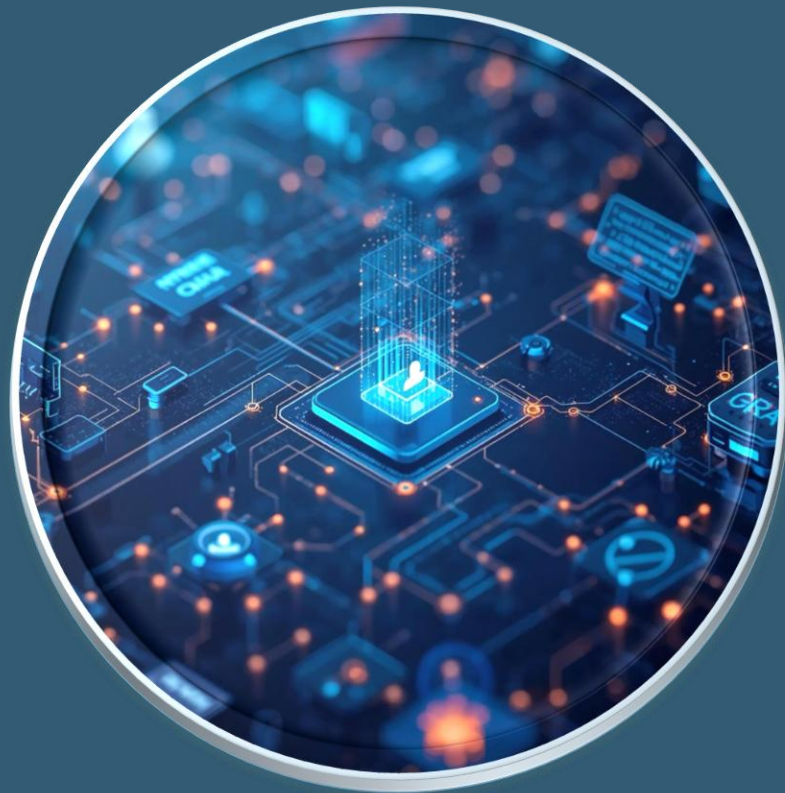




Unlock the Latest Updates on the CRA's Vulnerability Handling Harmonised Standard (R22a)



26 March 2026

Angelo D'Amato

Founder / Cybersecurity Expert @ Vulnir

Meet your speaker



Angelo D'Amato

Founder / Cybersecurity Expert @ Vulnir

Background

- With over fifteen years of experience, he is the subject matter expert for:
 - Cybersecurity assessments (Penetration testing, Security assessments)
 - Certifications (e.g., EN 303 645, IEC 62443, Common Criteria)
 - Regulatory compliance (e.g., Radio Equipment Directive, Cyber Resilience Act)
- I currently cover the role of rapporteur (*) for CRA as a CEN contractor within CEN/CLC/JTC 13/WG 9 for
 - PT2: Generic Security Requirements
 - PT3: Vulnerability handling requirements



* The European Union funds my activities within the STAN4CR project through the European Innovation Council and SMEs Executive Agency (EISMEA) under Grant Agreement No. 101196779.

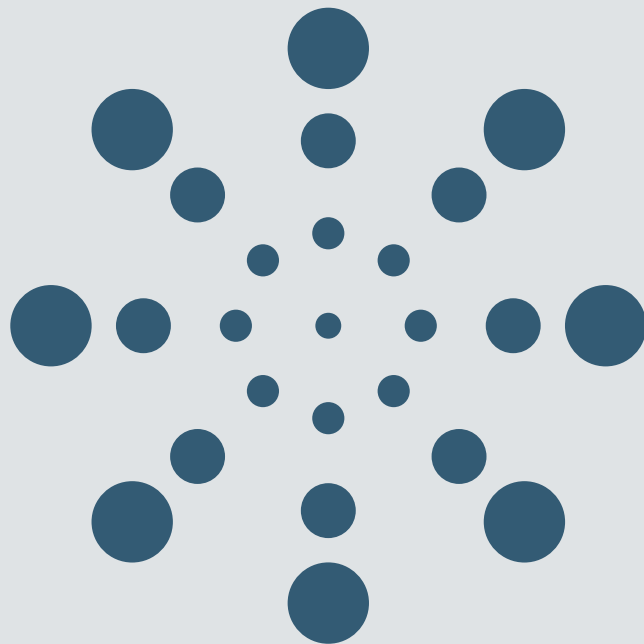
Agenda

- 01 Setting up the context
- 02 Outline of prEN 40000-1-3
- 03 Timeline and next steps
- 04 Q&A

01

Setting up the context

Vulnerability Handling & Disclosure



Modern Threats at Scale: Why Visibility & Patching Can't Wait

Fortinet's delayed alert on actively exploited defect put defenders at a disadvantage

The security vendor silently patched a vulnerability, but did not assign the flaw a CVE or publicly disclose its existence until 17 days later. By then, widespread attacks were already underway.

BY MATT KAPKO • NOVEMBER 17, 2025

Listen to this article 6:05 Learn more.



Fortinet office in Burnaby, BC, Canada, July 7, 2023. (Getty Images)

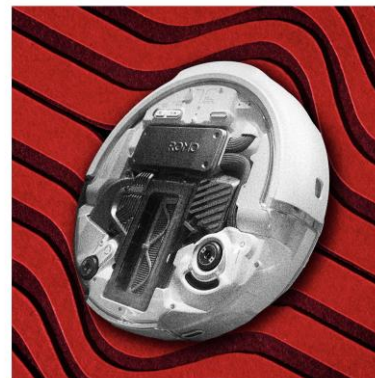
Source: CyberScoop (17 Nov 2025) - <https://cyberscoop.com/fortinet-delayed-disclosure-exploited-vulnerability/>

SHORT ORIGINATOR | SELF-HEAT-HEATING | HADDS-LEADING | SECURITY

FEB 26, 2026 9:30 AM

Security News This Week: Area Man Accidentally Hacks 6,700 Camera-Enabled Robot Vacuums

Plus: The top US cyber agency falls into shambles, AI models develop an upsetting penchant for nuclear weapons, and more.



Source: Wired (28 Feb 2026) - <https://www.wired.com/story/security-news-this-week-area-man-accidentally-hacks-6700-camera-enabled-robot-vacuums/>

NETWORK SECURITY

Hundreds of FortiGate Firewalls Hacked in AI-Powered Attacks: AWS

Threat actors relying on AI have been exploiting exposed ports and weak credentials to take over FortiGate devices.



By Jonut Arghire | February 23, 2026 (6:34 AM ET)



TRENDING

- 1 Navia Data Breach Impacts 2.7 Million
- 2 In Other News: New Android Safeguards, Operation Alice, UK Toughens Cyber Reporting
- 3 Critical Langflow Vulnerability Exploited Hours After Public Disclosure
- 4 Critical Quest KACE Vulnerability Potentially Exploited in Attacks
- 5 US Confirms Handala Link to Iran Government Amid 'Takedown of Hackers' Sites
- 6 3 Men Charged With Conspiring to Smuggle US Artificial Intelligence to China
- 7 Allure Security Raises \$17 Million for Online Brand Protection
- 8 Security Firm Aura Discloses Data Breach Impacting 900,000 Records

Over 600 Fortinet FortiGate firewall instances have been hacked in an AI-powered campaign that exploits exposed ports and weak credentials, AWS reports.

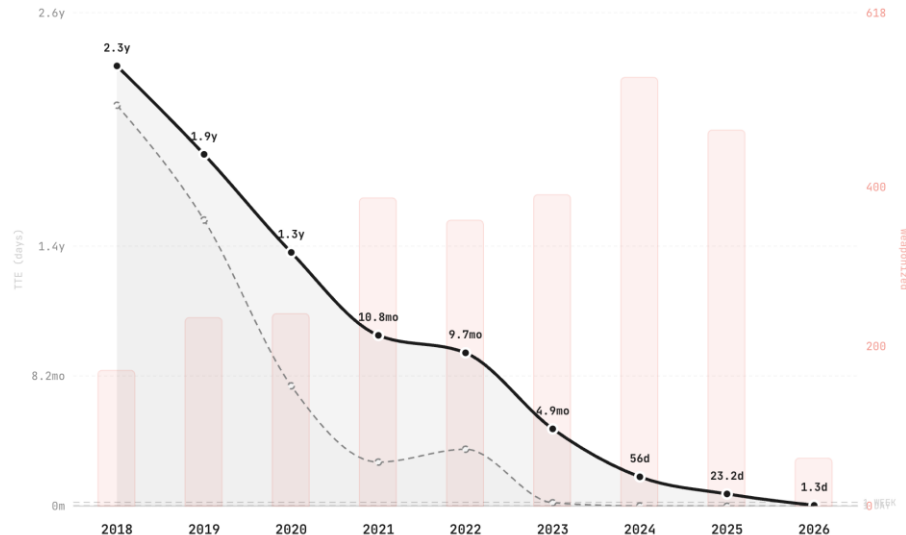
Source: SecurityWeek (23 Feb 2026) - <https://www.securityweek.com/hundreds-of-fortigate-firewalls-hacked-in-ai-powered-attacks-aws/>

Exploitation at Machine Speed

From Vulnerability to Exploitation

TTE (Time-to-Exploit) measures the gap between CVE disclosure and confirmed exploitation

— Mean TTE (10% trimmed, days) - - - Median TTE (days) ■ Weaponized Exploits (count)



Based on 3,520 CVE-exploit pairs from trusted sources (CISA KEV, VulnCheck KEV & XDB)

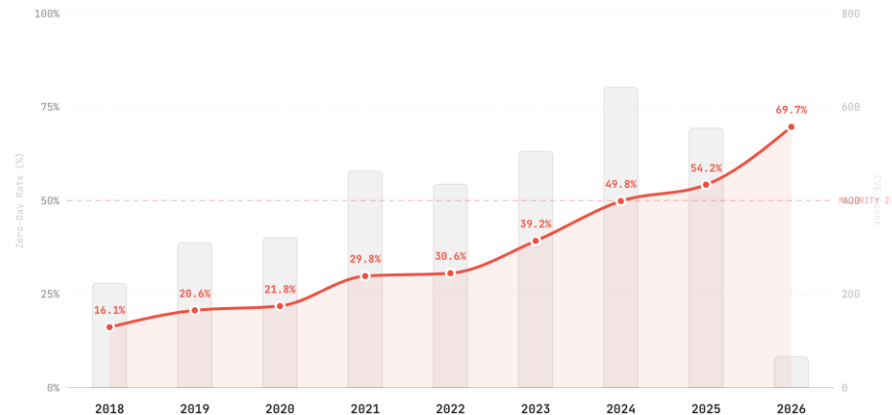
• zerodaycLock.com

Source: zerodaycLock.com (screenshots within this slide have been taken on 22nd March 2026)

Zero-Day Rate

Percentage of exploited CVEs where exploitation occurred before or on the day of disclosure (TTE ≤ 0)

— Zero-Day Rate (% of exploited) ■ Exploited CVEs (count)

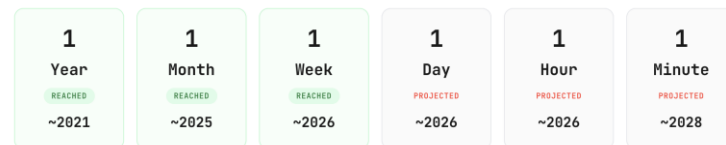


69.7% of exploited CVEs in 2026 are zero-days, up from 16.1% in 2018

• zerodaycLock.com

Time-to-Exploit Milestones

When mean time-to-exploit crosses each threshold

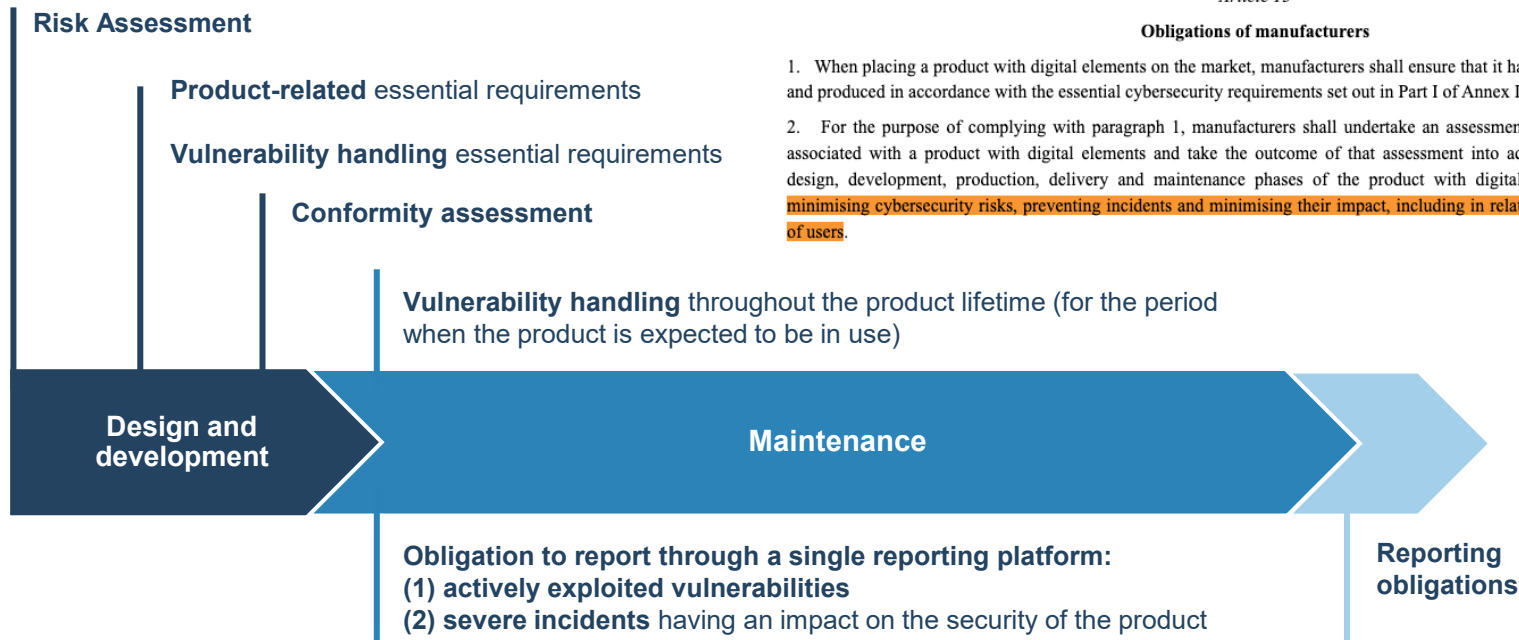


Obligations of manufacturers (CRA)

Article 13

Obligations of manufacturers

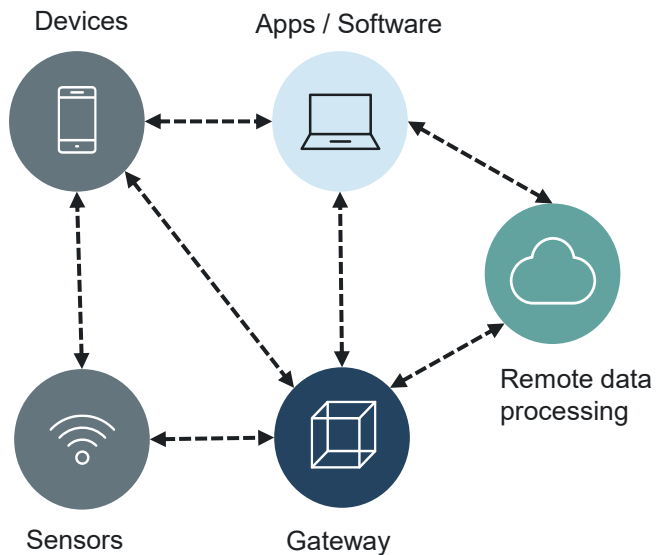
1. When placing a product with digital elements on the market, manufacturers shall ensure that it has been designed, developed and produced in accordance with the essential cybersecurity requirements set out in Part I of Annex I.
2. For the purpose of complying with paragraph 1, manufacturers shall undertake an assessment of the cybersecurity risks associated with a product with digital elements and take the outcome of that assessment into account during the planning, design, development, production, delivery and maintenance phases of the product with digital elements with a view to **minimising cybersecurity risks, preventing incidents and minimising their impact, including in relation to the health and safety of users.**



CRA Milestone - Time to prepare



Essential Requirements ANNEX I PART II VH



(1) ‘product with digital elements’ means a software or hardware product and its remote data processing solutions, including software or hardware components being placed on the market separately;

❑ Ensure that products with digital elements hardware and software placed on the EU market have fewer cybersecurity vulnerabilities.

❑ **Better protection** for consumers, supply chains, organisations, businesses, and IT Infrastructure

▪ **Secure by Design / Risk Assessment**

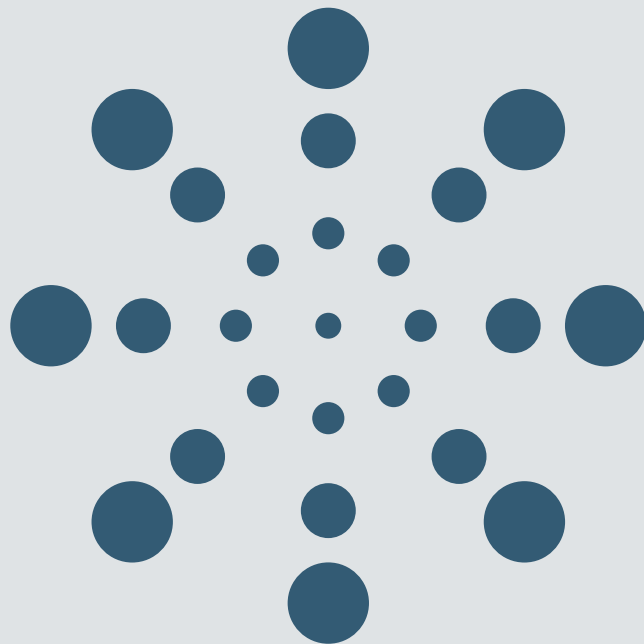
▪ **Vulnerability Handling Requirements**

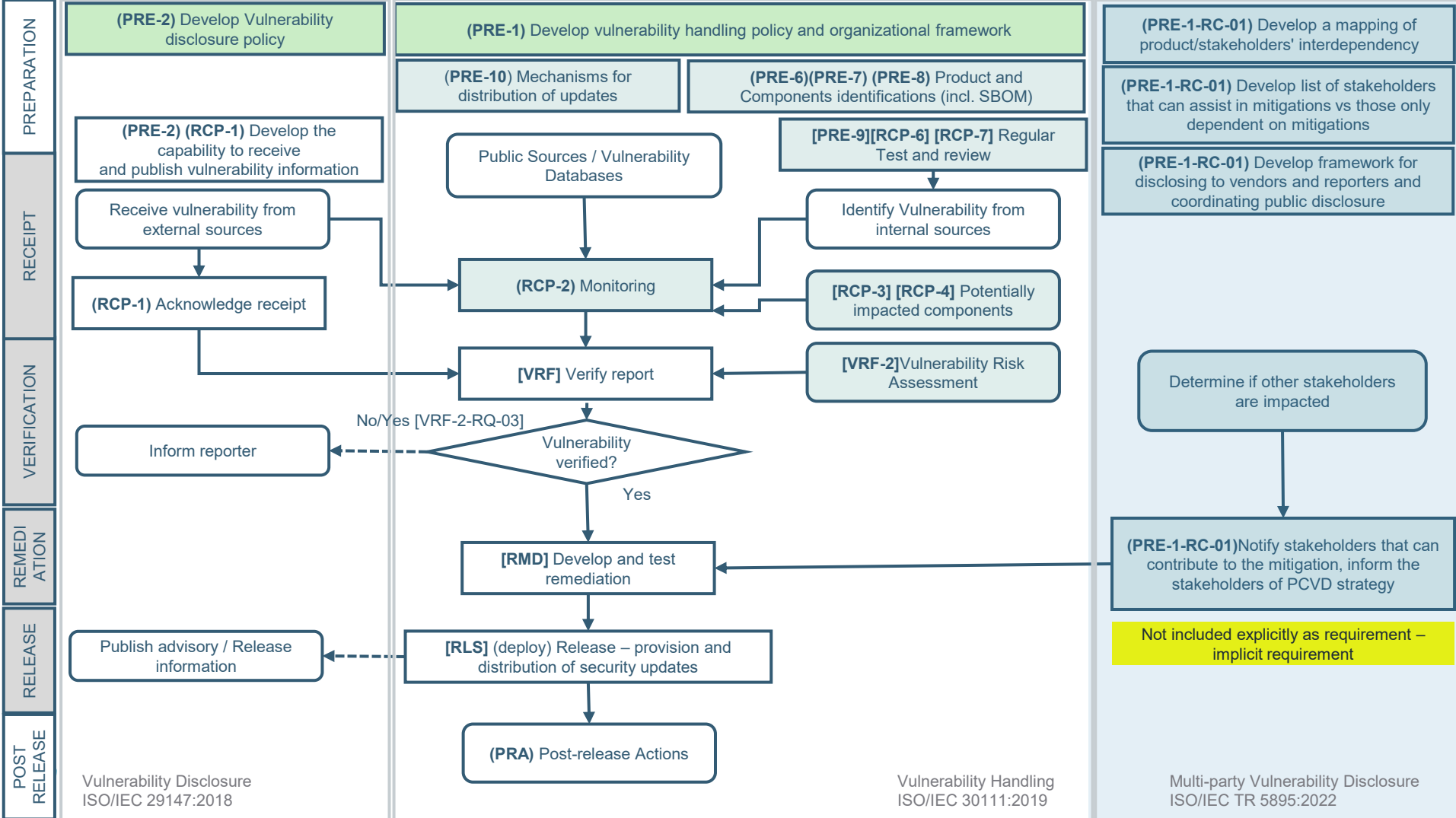
- Identify vulnerabilities / SBOM
- Remediate vulnerabilities
- Regular test
- Inform on fixed vulnerabilities
- CVD Policy in place
- Intake of potential vulnerabilities
- Secure distribution of updates
- Update available and related dissemination

02

Overview

prEN 40000-1-3



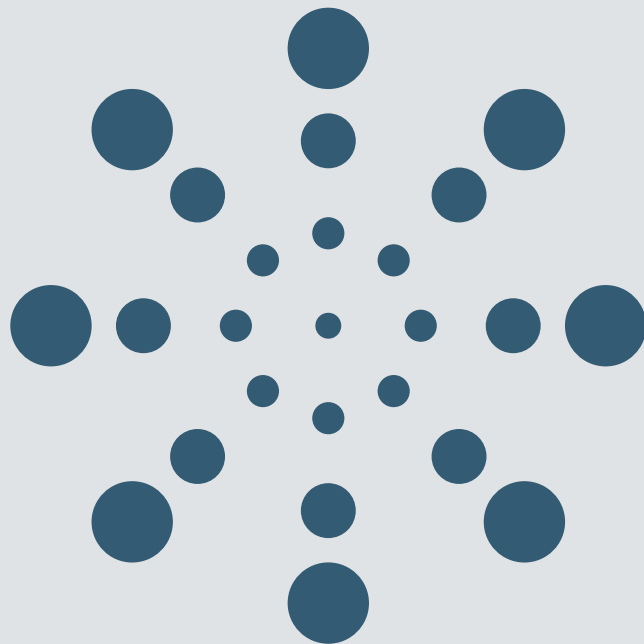


	LOW/MEDIUM CRITICAL PRODUCT	HIGH CRITICAL PRODUCT (vertical standards)
<u>Critical vulnerability</u>	More flexibility in resolution time and embargo period	Strict and well-defined timelines; horizontal standard cannot prescribe exact values but expects internal definition and adherence
<u>Secure communication</u>	It is desirable during the receipt of the vulnerability, but not mandatory	Mandatory; must not hinder accessibility or impede vulnerability reporting.
<u>Regular test and reviews</u>	Plan required, but it is non-prescriptive on how test cases and test methodologies are defined; flexibility in test case methods and execution. E.g. Run a vulnerability assessment.	More frequent and rigorous testing. Prescriptive plan required; E.g. includes manual testing, fuzzing, and formalized review processes This is implicit in how a manufacturer is defining their regular test and review plan
<u>SBOM</u>	Machine-readable format with at least top-level dependencies	Complete/ <i>transitive dependencies</i> in machine-readable format, as far as technically feasible More control over the supply chain
<u>SBOM Software component identifications</u>	Unique identifiers are desirable; no specific format is enforced (manufacturer-specific)	Mandatory machine-readable unique identifiers (e.g., CPE, PURL, SWHID); HASH enforcement.
<u>Advisories</u>	Machine-readable format is desirable.	Mandatory machine-readable format (e.g., CSAF)
<u>Post-release plan</u>	Post-release actions	Prescriptive expectations for continuous improvement and monitoring the effectiveness of the mitigations and <i>recurrence of security issues</i> .

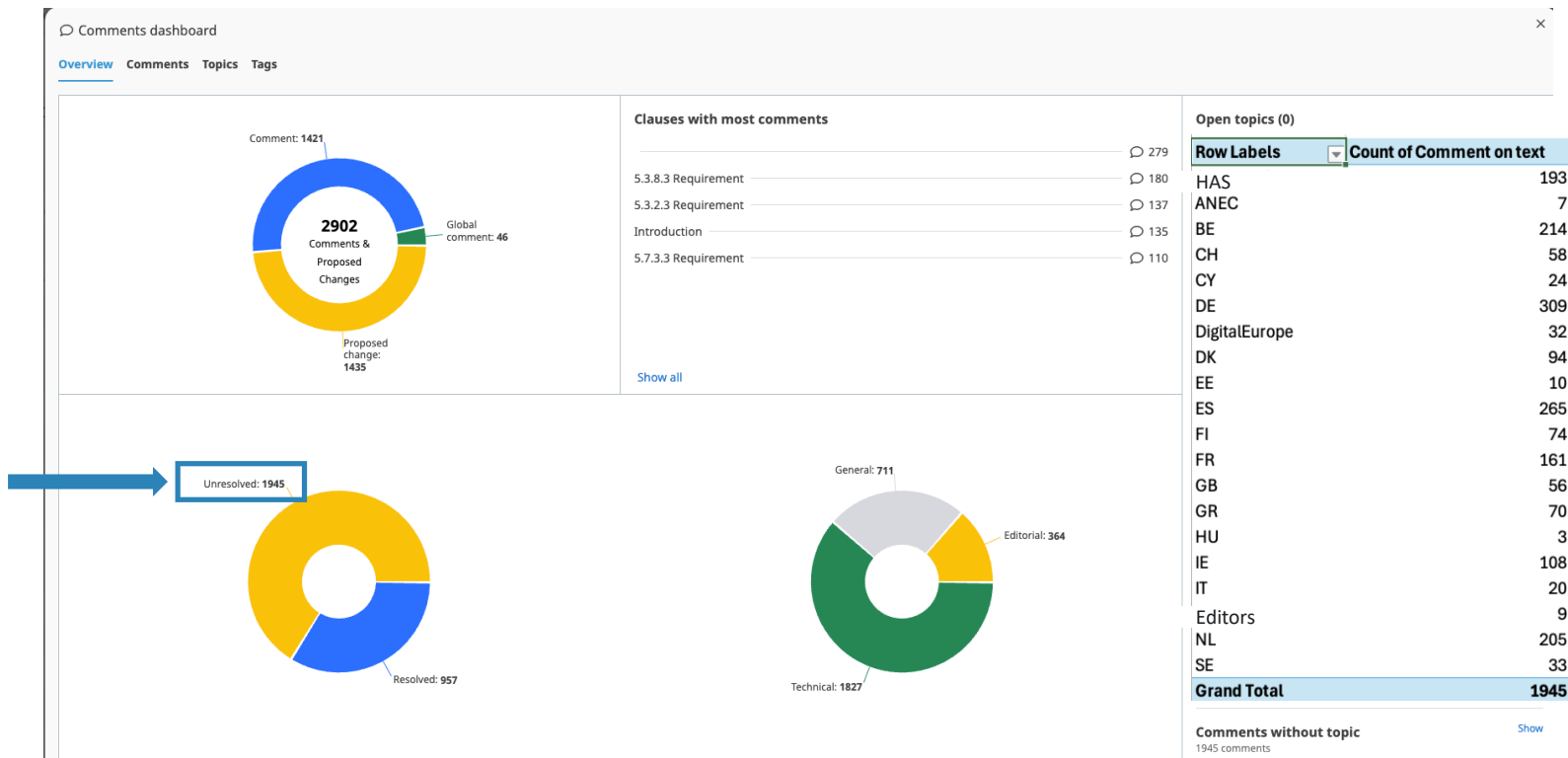
02

Updates

Comment Resolution phase



prEN 40000-1-3 Comment resolutions



HAS comments overview

Group of topic	Share of Comments	Summary
Risk-based sufficiency	~27%	Evidence, triad, Annex X
Multi-party CVD	~18%	Notifications, coordinator
SBOM	~15%	Licenses, identifiers, transitive
Distribution/Disclosure	~12%	Verification, EUVD phrasing
Verification/Triage	~10%	Intake, expedited
Remediation	~10%	Plan, RCA feedback
Accessibility/Comms	~8%	Accessible channels

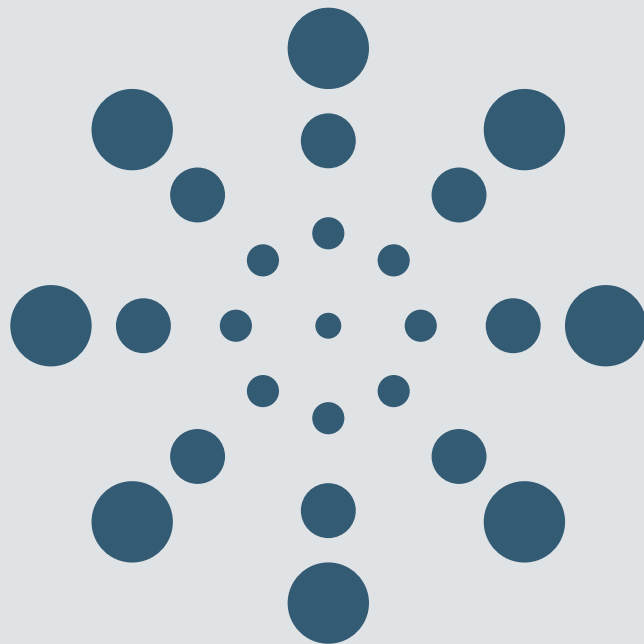
1. Stand-Alone PT3 & Normative References
2. Risk-Based Approach, Justification & Sufficiency
3. Multi-Party CVD & Supply-Chain Coordination
4. CVD Policy, Accessibility & Secure Communications
5. SBOM Content Completeness
6. Verification, Triage & Expedited Handling
7. Update Distribution & Disclosure
8. Remediation Planning, Testing & Root Cause Analysis Feedback
9. Terminology, Clarity & Editorial Issues
10. Annex ZA (Presumption of Conformity - Add RE explicitly)
11. Annex X (New Informative Annex) - Mapping with Risks

National Standards Body (NSB) comments overview

Topic	Concern	Views
Requirement Enhancements (RE)	Unclear, going beyond CRA mandate	Mostly want it refined, some want it removed
Risk-based approach & rigor	“Rigor” unclear, societal impact misused	Make systematic; priority only based on risk
Normative references	prEN 40000-1-2 normative dependency invalid	Make informative only
Conformity assessment	Unstructured, no sufficiency checks	Rebuild CA mapping with sufficiency and traceability
Separation of processes	VH mixed with testing	Split into separate clauses
Documentation burden	Too heavy, not risk-proportional	Scale to severity/impact
Policy content	Too detailed, product-specific	Simplify; remove stakeholder lists & SBOM input
Terminology	Hardware-centric, inconsistent	Modernize, centralize vocabulary
SBOM	Depth, hashes, transitive deps	CRA top-level only
MPCVD	Insufficient	Add explicit requirements
Publication	Machine-readable, EUVD references	Make optional/flexible
Evidence	Expectation unclear	Assess process, not instance
Structure	Figures/IDs confusing	Clarify, restructure

Timeline

Overview of the timelines for prEN 40000-1-3

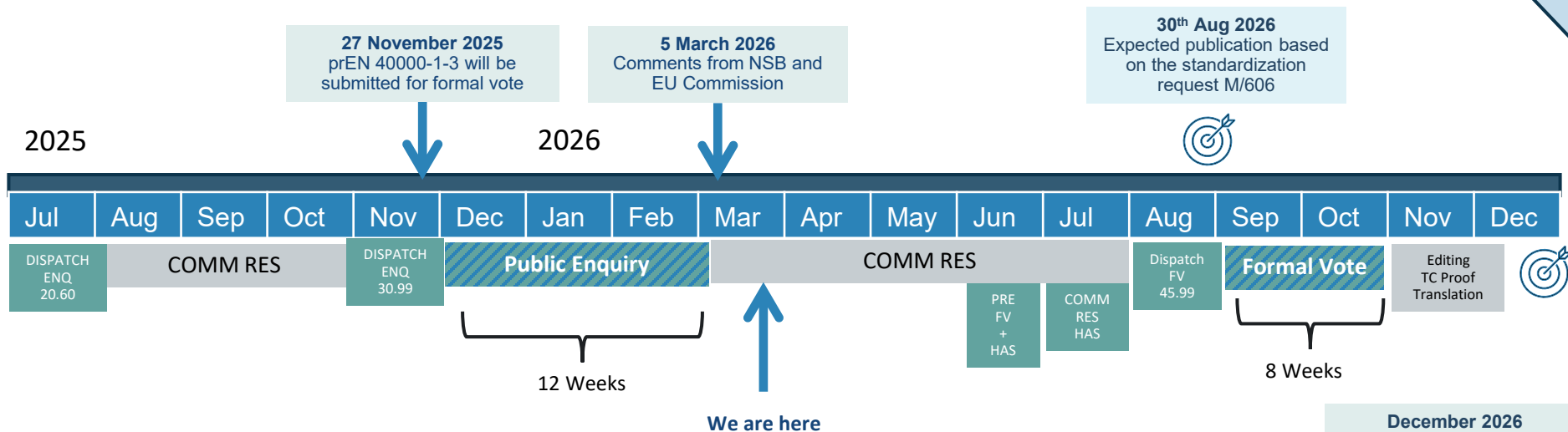


High level expected timeline (prEN 40000-1-3)



CENELEC

DRAFT
For discussion purposes only



December 2026
Estimated publication, but WG9 will do its best to speed up the comment resolution process to optimize as much as possible the timeline for delivery as requested by the EU Commission

04

Questions and Answers





Thank you

[VULNIR.com](https://vulnir.com)

info@vulnir.com