E DIN EN 40000-1-3:2026-02 (E)

Erscheinungsdatum: 2026-01-09

Cybersecurity requirements for products with digital elements - Part 1-3: Vulnerability Handling; English version prEN 40000-1-3:2025

Inhalt

Seite

European foreword 4

Introduction 5

1 Scope 7

2 Normative references 7

3 Terms and definitions 7

4 General 8
4.1 Structure of this document 8
4.2 Relationships with other international standards 9

5 Vulnerability handling 10
5.1 [APP] Applicability 10
5.1.1 General 10
5.1.2 [APP-1] Requirement enhancement applicability 10
5.2 [PRE] Preparation 11
5.2.1 General 11
5.2.2 [PRE-1] Policy on vulnerability handling 11
5.2.3 [PRE-2] Policy on coordinated vulnerability disclosure 13
5.2.4 [PRE-3] Operational security 15
5.2.5 [PRE-4] On-going communication 16
5.2.6 [PRE-5] Secure communication 17
5.2.7 [PRE-6] Product identification 18
5.2.8 PRE-7] Identification of software components 19
5.2.9 [PRE-8] Identification of hardware components 21
5.2.10 PRE-9] Planning regular test and reviews 22
5.2.11 PRE-10] Mechanisms for distribution 24
5.3 [RCP] Receipt 24
5.3.1 General 24
5.3.2 [RCP-1] Capability to receive reports 25
5.3.3 [RCP-2] Monitoring 26
5.3.4 [RCP-3] Potentially impacted software components 27
5.3.5 [RCP-4] Potentially impacted hardware components 27
5.3.6 [RCP-5] Coordinator involvement 28
5.3.7 [RCP-6] Performing regular tests 28
5.3.8 [RCP-7] Performing regular reviews 29
5.4 [VRF] Verification 30
5.4.1 General 30
5.4.2 [VRF-1] Initial assessment and verification 30
5.4.3 [VRF-2] Vulnerability risk assessment 32
5.5 [RMD] Remediation 33
5.5.1 General 33
5.5.2 [RMD-1] Remediation decision 33
5.5.3 [RMD-2] Remediation development 33
5.5.4 [RMD-3] Remediation Test 34
5.6 [RLS] Release 35
5.6.1 General 35
5.6.2 [RLS-1] Security update release 35

5.6.3 [RLS-2] Release Information **36**
5.7 [PRA] Post-release **38**
5.7.1 General **38**
5.7.2 [PRA-1] Post-release actions **38**

Annex ZA (informative) Relationship between this European Standard and the essential cybersecurity requirements of Regulation (EU) 2024/2847 of the European Parliament and of the Council of 23 October 2024 on horizontal cybersecurity requirements for products with digital elements and amending Regulations (EU) No 168/2013 and (EU) 2019/1020 and Directive (EU) 2020/1828 (Cyber Resilience Act) aimed to be covered **40**

Figures

Figure 1 — Vulnerability life cycle **6**

Figure 2 — Relationships between referred standards and this standard **9**

Tables

Table ZA.1 — Correspondence between [clause X of] this European Standard and Annex I of the Cyber Resilience Act **40**