



SLOVENSKI STANDARD

oSIST prEN 40000-1-3:2026

01-februar-2026

Zahteve za kibernetško varnost za izdelke z digitalnimi elementi - 1-3 del: Obravnavanje ranljivosti

Cybersecurity requirements for products with digital elements - Part 1-3: Vulnerability Handling

Cybersicherheitsanforderungen für Produkte mit digitalen Bestandteilen - Umgang mit Schwachstellen

iTeh Standards
(<https://standards.iteh.ai>)
Document Preview

Ta slovenski standard je istoveten z: prEN 40000-1-3

~~oSIST prEN 40000-1-3:2026~~

<https://standards.iteh.ai/catalog/standards/sist/adc84987-2c6e-4c2a-9e9e-817773a42891/osist-pren-40000-1-3-2026>

ICS:

35.030

Informacijska varnost

IT Security

oSIST prEN 40000-1-3:2026

en,fr,de

EUROPEAN STANDARD
NORME EUROPÉENNE
EUROPÄISCHE NORM

DRAFT
prEN 40000-1-3

December 2025

ICS 35.030

English version

Cybersecurity requirements for products with digital elements - Part 1-3: Vulnerability Handling

Cybersicherheitsanforderungen für Produkte mit digitalen Bestandteilen - Umgang mit Schwachstellen

This draft European Standard is submitted to CEN members for enquiry. It has been drawn up by the Technical Committee CEN/CLC/JTC 13.

If this draft becomes a European Standard, CEN and CENELEC members are bound to comply with the CEN/CENELEC Internal Regulations which stipulate the conditions for giving this European Standard the status of a national standard without any alteration.

This draft European Standard was established by CEN and CENELEC in three official versions (English, French, German). A version in any other language made by translation under the responsibility of a CEN and CENELEC member into its own language and notified to the CEN-CENELEC Management Centre has the same status as the official versions.

CEN and CENELEC members are the national standards bodies and national electrotechnical committees of Austria, Belgium, Bulgaria, Croatia, Cyprus, Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Iceland, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, Netherlands, Norway, Poland, Portugal, Republic of North Macedonia, Romania, Serbia, Slovakia, Slovenia, Spain, Sweden, Switzerland, Türkiye and United Kingdom.

Recipients of this draft are invited to submit, with their comments, notification of any relevant patent rights of which they are aware and to provide supporting documentation. Recipients of this draft are invited to submit, with their comments, notification of any relevant patent rights of which they are aware and to provide supporting documentation.

Warning : This document is not a European Standard. It is distributed for review and comments. It is subject to change without notice and shall not be referred to as a European Standard.



**CEN-CENELEC Management Centre:
Rue de la Science 23, B-1040 Brussels**

Contents	Page
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	8
5 Vulnerability handling	9
5.1 General	9
5.2 [APP] Applicability	9
5.2.1 General	10
5.2.2 [APP-1] Requirement enhancement applicability	10
5.3 [PRE] Preparation	10
5.3.1 General	10
5.3.2 [PRE-1] Policy on vulnerability handling	10
5.3.3 [PRE-2] Policy on coordinated vulnerability disclosure	12
5.3.4 [PRE-3] Operational security	14
5.3.5 [PRE-4] On-going communication	15
5.3.6 [PRE-5] Secure communication	16
5.3.7 [PRE-6] Product identification	17
5.3.8 [PRE-7] Identification of software components	18
5.3.9 [PRE-8] Identification of hardware components	20
5.3.10 [PRE-9] Planning regular test and reviews	21
5.3.11 [PRE-10] Mechanisms for distribution	22
5.4 [RCP] Receipt	22
5.4.1 General	22
5.4.2 [RCP-1] Capability to receive reports	23
5.4.3 [RCP-2] Monitoring	24
5.4.4 [RCP-3] Potentially impacted software components	25
5.4.5 [RCP-4] Potentially impacted hardware components	25
5.4.6 [RCP-5] Coordinator involvement	26
5.4.7 [RCP-6] Performing regular tests	26
5.4.8 [RCP-7] Performing regular reviews	27
5.5 [VRF] Verification	28
5.5.1 General	28
5.5.2 [VRF-1] Initial assessment and verification	28
5.5.3 [VRF-2] Vulnerability risk assessment	29
5.6 [RMD] Remediation	30
5.6.1 General	30
5.6.2 [RMD-1] Remediation decision	30
5.6.3 [RMD-2] Remediation development	30
5.6.4 [RMD-3] Remediation test	31
5.7 [RLS] Release	32
5.7.1 General	32
5.7.2 [RLS-1] Security update release	32
5.7.3 [RLS-2] Release information	33
5.8 [PRA] Post-release	35
5.8.1 General	35
5.8.2 [PRA-1] Post-release actions	35

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	36
Bibliography	37

iTeh Standards
(<https://standards.iteh.ai>)
Document Preview

[oSIST prEN 40000-1-3:2026](https://standards.iteh.ai/catalog/standards/sist/adc84987-2c6e-4c2a-9e9e-817773a42891/osist-pren-40000-1-3-2026)

<https://standards.iteh.ai/catalog/standards/sist/adc84987-2c6e-4c2a-9e9e-817773a42891/osist-pren-40000-1-3-2026>