ICS 33.060.20 SLOVENSKÁ TECHNICKÁ NORMA December 2024

STN	**Spoločné bezpečnostné požiadavky pre rádiové zariadenia Časť 2: Rádiové zariadenia spracúvajúce údaje, menovite rádiové zariadenia pripojené na internet, rádiové zariadenia pre starostlivosť o deti, rádiové zariadenia hračiek a nositeľné rádiové zariadenia**	**STN EN 18031-2** 97 4191

Common security requirements for radio equipment - Part 2: radio equipment processing data, namely Internet connected radio equipment, childcare radio equipment, toys radio equipment and wearable radio equipment

Táto norma obsahuje anglickú verziu európskej normy.
This standard includes the English version of the European Standard.

Táto norma bola oznámená vo Vestníku ÚNMS SR č. 11/24

Obsahuje: EN 18031-2:2024

obsahuje farebné strany

139452

EUROPEAN STANDARD **EN 18031-2**

NORME EUROPÉENNE

EUROPÄISCHE NORM August 2024

ICS 33.060.20

English version

Common security requirements for radio equipment - Part 2: radio equipment processing data, namely Internet connected radio equipment, childcare radio equipment, toys radio equipment and wearable radio equipment

Exigences de sécurité communes applicables aux équipements radioélectriques - Partie 2 : Équipements radioélectriques qui traitent des données, à savoir les équipements radioélectriques connectés à l'internet, les équipements radioélectriques destinés à la garde d'enfants, les jouets dotés d'équipements radioélectriques et les équipements radioélectriques portables

Gemeinsame Sicherheitsanforderungen für datenverarbeitende Funkanlagen, namentlich mit dem Internet verbundene Funkanlagen, in der Kinderbetreuung eingesetzte Funkanlagen, in Spielzeug eingesetzte Funkanlagen sowie an einem Teil des menschlichen Körpers oder an Kleidungsstücken getragene Funkanlagen

This European Standard was approved by CEN on 1 August 2024.

Contents

Page

European foreword

This document (EN 18031-2:2024) has been prepared by Technical Committee CEN/CENELEC JTC 13 “Cybersecurity and Data Protection”, the secretariat of which is held by DIN.

This European Standard shall be given the status of a national standard, either by publication of an identical text or by endorsement, at the latest by February 2025, and conflicting national standards shall be withdrawn at the latest by February 2025.

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights. CEN shall not be held responsible for identifying any or all such patent rights.

This document has been prepared under a standardization request addressed to CEN-CENELEC by the European Commission. The Standing Committee of the EFTA States subsequently approves these requests for its Member States.

For the relationship with EU Legislation, see informative Annex ZA, which is an integral part of this document.

Any feedback and questions on this document should be directed to the users’ national standards body. A complete listing of these bodies can be found on the CEN website.

According to the CEN-CENELEC Internal Regulations, the national standards organisations of the following countries are bound to implement this European Standard: 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 the United Kingdom.

Introduction

Vigilance is required from manufacturers to improve the overall resilience against cybersecurity threats caused by the increased connectivity of radio equipment [36] and the growing ability of malicious threat actors to cause harm to users, organizations, and society.

The security requirements presented in this baseline standard are developed to improve the ability of radio equipment to protect its security and privacy assets against common cybersecurity threats and to mitigate publicly known exploitable vulnerabilities.

It is important to note that to achieve the overall cybersecurity of radio equipment, defence in depth best practices will be needed by both the manufacturer and user. In particular, no single measure will suffice to achieve the given objectives, indeed achieving even a single security objective will usually require a suite of mechanisms and measures. Throughout this document, the guidance material includes lists of examples. These examples given are only indicative possibilities, as there are other possibilities that are not listed, and even using the examples given will not be sufficient unless the mechanisms and measures chosen are implemented in a coordinated fashion.

1 Scope

This document specifies common security requirements and related assessment criteria for radio equipment [36] processing personal data [40] or traffic data [41] or location data [41] for either internet connected radio equipment [37], radio equipment designed or intended exclusively for childcare [37]; toys [39] and wearable radio equipment [37] (hereinafter referred to as "equipment").

2 Normative references

There are no normative references in this document.