

Information technology - Security techniques -
Vulnerability handling processes (ISO/IEC 30111:2019)

EESTI STANDARDI EESSÕNA

NATIONAL FOREWORD

See Eesti standard EVS-EN ISO/IEC 30111:2020 sisaldab Euroopa standardi EN ISO/IEC 30111:2020 ingliskeelset teksti.	This Estonian standard EVS-EN ISO/IEC 30111:2020 consists of the English text of the European standard EN ISO/IEC 30111:2020.
Standard on jõustunud sellekohase teate avaldamisega EVS Teatajas.	This standard has been endorsed with a notification published in the official bulletin of the Estonian Centre for Standardisation.
Euroopa standardimisorganisatsioonid on teinud Euroopa standardi rahvuslikele liikmetele kättesaadavaks 27.05.2020.	Date of Availability of the European standard is 27.05.2020.
Standard on kättesaadav Eesti Standardikeskusest.	The standard is available from the Estonian Centre for Standardisation.

Tagasisidet standardi sisu kohta on võimalik edastada, kasutades EVS-i veebilehel asuvat tagasiside vormi või saates e-kirja meiliaadressile standardiosakond@evs.ee.

ICS 35.030

Standardite reprodutseerimise ja levitamise õigus kuulub Eesti Standardikeskusele

Andmete paljundamine, taastekitamine, kopeerimine, salvestamine elektroonsesse süsteemi või edastamine ükskõik millises vormis või millisel teel ilma Eesti Standardikeskuse kirjaliku loata on keelatud.

Kui Teil on küsimusi standardite autorikaitse kohta, võtke palun ühendust Eesti Standardikeskusega:
Koduleht www.evs.ee; telefon 605 5050; e-post info@evs.ee

The right to reproduce and distribute standards belongs to the Estonian Centre for Standardisation

No part of this publication may be reproduced or utilized in any form or by any means, electronic or mechanical, including photocopying, without a written permission from the Estonian Centre for Standardisation.

If you have any questions about copyright, please contact Estonian Centre for Standardisation:

Homepage www.evs.ee; phone +372 605 5050; e-mail info@evs.ee

English version

Information technology - Security techniques - Vulnerability handling processes (ISO/IEC 30111:2019)

Technologies de l'information - Techniques de sécurité
- Processus de traitement de la vulnérabilité (ISO/IEC
30111:2019)

Informationstechnik - IT-Sicherheitsverfahren -
Prozesse für die Behandlung von Schwachstellen
(ISO/IEC 30111:2019)

This European Standard was approved by CEN on 3 May 2020.

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. Up-to-date lists and bibliographical references concerning such national standards may be obtained on application to the CEN-CENELEC Management Centre or to any CEN and CENELEC member.

This European Standard exists 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, Turkey and United Kingdom.



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

European foreword

The text of ISO/IEC 30111:2019 has been prepared by Technical Committee ISO/IEC JTC 1 "Information technology" of the International Organization for Standardization (ISO) and has been taken over as EN ISO/IEC 30111:2020 by Technical Committee CEN/CLC/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 November 2020, and conflicting national standards shall be withdrawn at the latest by November 2020.

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.

According to the CEN-CENELEC Internal Regulations, the national standards organizations 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, Turkey and the United Kingdom.

Endorsement notice

The text of ISO/IEC 30111:2019 has been approved by CEN as EN ISO/IEC 30111:2020 without any modification.

Contents

Page

Foreword	iv
Introduction	v
1 Scope	1
2 Normative references	1
3 Terms and definitions	1
4 Abbreviated terms	1
5 Relationships to other International Standards	1
5.1 ISO/IEC 29147	1
5.2 ISO/IEC 27034 (all parts)	2
5.3 ISO/IEC 27036-3	2
5.4 ISO/IEC 15408-3	3
6 Policy and organizational framework	3
6.1 General	3
6.2 Leadership	3
6.2.1 Leadership and commitment	3
6.2.2 Policy	3
6.2.3 Organizational roles, responsibilities, and authorities	4
6.3 Vulnerability handling policy development	4
6.4 Organizational framework development	4
6.5 Vendor CSIRT or PSIRT	5
6.5.1 General	5
6.5.2 PSIRT mission	5
6.5.3 PSIRT responsibilities	5
6.5.4 Staff capabilities	6
6.6 Responsibilities of the product business division	6
6.7 Responsibilities of customer support and public relations	7
6.8 Legal consultation	7
7 Vulnerability handling process	7
7.1 Vulnerability handling phases	7
7.1.1 General	7
7.1.2 Preparation	8
7.1.3 Receipt	8
7.1.4 Verification	9
7.1.5 Remediation development	10
7.1.6 Release	10
7.1.7 Post-release	10
7.2 Process monitoring	11
7.3 Confidentiality of vulnerability information	11
8 Supply chain considerations	11
Bibliography	13

Foreword

ISO (the International Organization for Standardization) and IEC (the International Electrotechnical Commission) form the specialized system for worldwide standardization. National bodies that are members of ISO or IEC participate in the development of International Standards through technical committees established by the respective organization to deal with particular fields of technical activity. ISO and IEC technical committees collaborate in fields of mutual interest. Other international organizations, governmental and non-governmental, in liaison with ISO and IEC, also take part in the work.

The procedures used to develop this document and those intended for its further maintenance are described in the ISO/IEC Directives, Part 1. In particular, the different approval criteria needed for the different types of document should be noted. This document was drafted in accordance with the editorial rules of the ISO/IEC Directives, Part 2 (see www.iso.org/directives).

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights. ISO and IEC shall not be held responsible for identifying any or all such patent rights. Details of any patent rights identified during the development of the document will be in the Introduction and/or on the ISO list of patent declarations received (see www.iso.org/patents) or the IEC list of patent declarations received (see <http://patents.iec.ch>).

Any trade name used in this document is information given for the convenience of users and does not constitute an endorsement.

For an explanation of the voluntary nature of standards, the meaning of ISO specific terms and expressions related to conformity assessment, as well as information about ISO's adherence to the World Trade Organization (WTO) principles in the Technical Barriers to Trade (TBT) see www.iso.org/iso/foreword.html.

This document was prepared by Joint Technical Committee ISO/IEC JTC 1, *Information technology*, Subcommittee SC 27, *Information security, cybersecurity and privacy protection*.

Any feedback or questions on this document should be directed to the user's national standards body. A complete listing of these bodies can be found at www.iso.org/members.html.

This second edition cancels and replaces the first edition (ISO/IEC 30111:2013), which has been technically revised. The main changes compared to the previous edition are as follows:

- a number of normative provisions have been revised or added (summarized in Annex A);
- organizational and editorial changes have been made for clarity and harmonization with ISO/IEC 29147:2018.

This document is intended to be used with ISO/IEC 29147.

Introduction

This document describes processes for vendors to handle reports of potential vulnerabilities in products and services.

The audience for this document includes developers, vendors, evaluators, and users of information technology products and services. The following audiences can use this document:

- developers and vendors, when responding to actual or potential vulnerability reports;
- evaluators, when assessing the security assurance afforded by vendors' and developers' vulnerability handling processes; and
- users, to express procurement requirements to developers, vendors and integrators.

This document is integrated with ISO/IEC 29147 at the point of receiving potential vulnerability reports and at the point of distributing vulnerability remediation information (see [5.1](#)).

Relationships to other standards are noted in [Clause 5](#).

Information technology — Security techniques — Vulnerability handling processes

1 Scope

This document provides requirements and recommendations for how to process and remediate reported potential vulnerabilities in a product or service.

This document is applicable to vendors involved in handling vulnerabilities.

2 Normative references

The following documents are referred to in the text in such a way that some or all of their content constitutes requirements of this document. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

ISO/IEC 27000, *Information technology — Security techniques — Information security management systems — Overview and vocabulary*

ISO/IEC 29147:2018, *Information technology — Security techniques — Vulnerability disclosure*

3 Terms and definitions

For the purposes of this document, terms and definitions given in ISO/IEC 27000 and ISO/IEC 29147 apply.

ISO and IEC maintain terminological databases for use in standardization at the following addresses:

- ISO Online browsing platform: available at <https://www.iso.org/obp>
- IEC Electropedia: available at <http://www.electropedia.org/>

4 Abbreviated terms

The following abbreviated terms are used in this document.

CSIRT Computer Security Incident Response Team

PSIRT Product Security Incident Response Team

5 Relationships to other International Standards

5.1 ISO/IEC 29147

ISO/IEC 29147 shall be used in conjunction with this document. The relationship between the two is illustrated in [Figure 1](#).

This document provides guidelines for vendors on how to process and remediate potential vulnerability information reported by internal or external individuals or organizations.

ISO/IEC 29147 provides guidelines for vendors to include in their normal business processes when receiving reports about potential vulnerabilities from external individuals or organizations and when distributing vulnerability remediation information to affected users.