INTERNATIONAL STANDARD

ISO/IEC 30111

Second edition
2019-10

Information technology — Security techniques — Vulnerability handling processes

Technologies de l'information — Techniques de sécurité — Processus de traitement de la vulnérabilité

Reference number
ISO/IEC 30111:2019(E)

ISO copyright office
CP 401 • Ch. de Blandonnet 8
CH-1214 Vernier, Geneva
Phone: +41 22 749 01 11
Fax: +41 22 749 09 47
Email: copyright@iso.org
Website: www.iso.org

Published in Switzerland

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.