INTERNATIONAL STANDARD

ISO/IEC 29147

Second edition
2018-10

Information technology — Security techniques — Vulnerability disclosure

Technologies de l'information — Techniques de sécurité — Divulgation de vulnérabilité

Reference number
ISO/IEC 29147:2018(E)

COPYRIGHT PROTECTED DOCUMENT

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 vi

Introduction vii

1 Scope 1

2 Normative references 1

3 Terms and definitions 1

4 Abbreviated terms 3

5 Concepts 3

5.1 General 3
5.2 Structure of this document 3
5.3 Relationships to other International Standards 4
5.3.1 ISO/IEC 30111 4
5.3.2 ISO/IEC 27002 5
5.3.3 ISO/IEC 27034 series 6
5.3.4 ISO/IEC 27036-3 6
5.3.5 ISO/IEC 27017 6
5.3.6 ISO/IEC 27035 series 6
5.3.7 Security evaluation, testing and specification 6
5.4 Systems, components, and services 6
5.4.1 Systems 6
5.4.2 Components 6
5.4.3 Products 6
5.4.4 Services 7
5.4.5 Vulnerability 7
5.4.6 Product interdependency 7
5.5 Stakeholder roles 8
5.5.1 General 8
5.5.2 User 8
5.5.3 Vendor 8
5.5.4 Reporter 8
5.5.5 Coordinator 9
5.6 Vulnerability handling process summary 9
5.6.1 General 9
5.6.2 Preparation 10
5.6.3 Receipt 10
5.6.4 Verification 11
5.6.5 Remediation development 11
5.6.6 Release 11
5.6.7 Post-release 12
5.6.8 Embargo period 12
5.7 Information exchange during vulnerability disclosure 12
5.8 Confidentiality of exchanged information 13
5.8.1 General 13
5.8.2 Secure communications 13
5.9 Vulnerability advisories 13
5.10 Vulnerability exploitation 14
5.11 Vulnerabilities and risk 14

6 Receiving vulnerability reports 14

6.1 General 14
6.2 Vulnerability reports 14
6.2.1 General 14
6.2.2 Capability to receive reports 14
6.2.3 Monitoring 15

6.2.4 Report tracking 15
6.2.5 Report acknowledgement 15
6.3 Initial assessment 16
6.4 Further investigation 16
6.5 On-going communication 16
6.6 Coordinator involvement 16
6.7 Operational security 17

7 Publishing vulnerability advisories 17
7.1 General 17
7.2 Advisory 17
7.3 Advisory publication timing 17
7.4 Advisory elements 18
7.4.1 General 18
7.4.2 Identifiers 18
7.4.3 Date and time 18
7.4.4 Title 19
7.4.5 Overview 19
7.4.6 Affected products 19
7.4.7 Intended audience 19
7.4.8 Localization 19
7.4.9 Description 19
7.4.10 Impact 19
7.4.11 Severity 20
7.4.12 Remediation 20
7.4.13 References 20
7.4.14 Credit 20
7.4.15 Contact information 20
7.4.16 Revision history 20
7.4.17 Terms of use 20
7.5 Advisory communication 20
7.6 Advisory format 21
7.7 Advisory authenticity 21
7.8 Remediations 21
7.8.1 General 21
7.8.2 Remediation authenticity 21
7.8.3 Remediation deployment 21

8 Coordination 21
8.1 General 21
8.2 Vendors playing multiple roles 22
8.2.1 General 22
8.2.2 Vulnerability reporting among vendors 22
8.2.3 Reporting vulnerability information to other vendors 22

9 Vulnerability disclosure policy 22
9.1 General 22
9.2 Required policy elements 23
9.2.1 General 23
9.2.2 Preferred contact mechanism 23
9.3 Recommended policy elements 23
9.3.1 General 23
9.3.2 Vulnerability report contents 23
9.3.3 Secure communication options 24
9.3.4 Setting communication expectations 24
9.3.5 Scope 24
9.3.6 Publication 24
9.3.7 Recognition 24
9.4 Optional policy elements 24
9.4.1 General 24

9.4.2 Legal considerations 24
9.4.3 Disclosure timeline 24

Annex A (informative) **Example vulnerability disclosure policies** **25**

Annex B (informative) **Information to request in a report** **26**

Annex C (informative) **Example advisories** **27**

Annex D (informative) **Summary of normative elements** **30**

Bibliography **32**

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, *Security techniques*.

This second edition cancels and replaces the first edition (ISO/IEC 29147:2014), which has been technically revised.

The main changes compared to the previous edition are as follows:

— a number of normative provisions have been added (summarized in Annex D);

— numerous organizational and editorial changes have been made for clarity.

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 document is intended to be used with ISO/IEC 30111.

Introduction

In the contexts of information technology and cybersecurity, a vulnerability is a behaviour or set of conditions present in a system, product, component, or service that violates an implicit or explicit security policy. A vulnerability can be thought of as a weakness or exposure that allows a security impact or consequence. Attackers exploit vulnerabilities to compromise confidentiality, integrity, availability, operation, or some other security property.

Vulnerabilities often result from failures of a program or system to securely handle untrusted or unexpected input. Causes that lead to vulnerabilities include errors in coding or configuration, oversights in design choices, and insecure protocol and format specifications.

Despite significant efforts to improve software security, modern software and systems are so complex that it is impractical to produce them without vulnerabilities. Risk factors of vulnerabilities include:

— operating and relying on systems that have known vulnerabilities;

— not having sufficient information about vulnerabilities;

— not knowing that vulnerabilities exist.

This document describes vulnerability disclosure: techniques and policies for vendors to receive vulnerability reports and publish remediation information. Vulnerability disclosure enables both the remediation of vulnerabilities and better-informed risk decisions. Vulnerability disclosure is a critical element of the support, maintenance, and operation of any product or service that is exposed to active threats. This includes practically any product or service that uses open networks such as the Internet. A vulnerability disclosure capability is an essential part of the development, acquisition, operation, and support of all products and services. Operating without vulnerability disclosure capability puts users at increased risk.

The term "vulnerability disclosure" is used to describe the overall activities associated with receiving vulnerability reports and providing remediation information. Additional activities such as investigating and prioritizing reports, developing, testing, and deploying remediations, and improving secure development are called "vulnerability handling" and are described in ISO/IEC 30111. The term "disclosure" is also used more narrowly to mean the act of informing a party about a vulnerability for the first time (see 3.2).

Major goals of vulnerability disclosure include:

— reducing risk by remediating vulnerabilities and informing users;

— minimizing harm and cost associated with the disclosure;

— providing users with sufficient information to evaluate risk due to vulnerabilities;

— setting expectations to facilitate cooperative interaction and coordination among stakeholders.

The processes described in this document aim to minimize risk, cost, and harm to all stakeholders. Due to the volume of reported vulnerabilities, lack of accurate and complete information, and other factors involved, it is not possible to create a single, fixed process that applies to every disclosure event.

The normative elements in this document provide minimum requirements to create a functional vulnerability disclosure capability. Vendors should adapt the additional informative guidance in this document to fit their particular needs and those of users and other stakeholders.

Information technology — Security techniques — Vulnerability disclosure

1 Scope

This document provides requirements and recommendations to vendors on the disclosure of vulnerabilities in products and services. Vulnerability disclosure enables users to perform technical vulnerability management as specified in ISO/IEC 27002:2013, 12.6.1[1]. Vulnerability disclosure helps users protect their systems and data, prioritize defensive investments, and better assess risk. The goal of vulnerability disclosure is to reduce the risk associated with exploiting vulnerabilities. Coordinated vulnerability disclosure is especially important when multiple vendors are affected. This document provides:

- guidelines on receiving reports about potential vulnerabilities;
- guidelines on disclosing vulnerability remediation information;
- terms and definitions that are specific to vulnerability disclosure;
- an overview of vulnerability disclosure concepts;
- techniques and policy considerations for vulnerability disclosure;
- examples of techniques, policies (Annex A), and communications (Annex B).

Other related activities that take place between receiving and disclosing vulnerability reports are described in ISO/IEC 30111.

This document is applicable to vendors who choose to practice vulnerability disclosure to reduce risk to users of vendors' products and services.

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 30111, *Information technology — Security techniques — Vulnerability handling processes*