INTERNATIONAL STANDARD

ISO/IEC 30111

First edition
2013-11-01

Information technology — Security techniques — Vulnerability handling processes

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

Reference number
ISO/IEC 30111:2013(E)

ISO copyright office
Case postale 56 • CH-1211 Geneva 20
Tel. + 41 22 749 01 11
Fax + 41 22 749 09 47
E-mail copyright@iso.org
Web www.iso.org

Published in Switzerland

Contents

Page

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. In the field of information technology, ISO and IEC have established a joint technical committee, ISO/IEC JTC 1.

International Standards are drafted in accordance with the rules given in the ISO/IEC Directives, Part 2.

The main task of the joint technical committee is to prepare International Standards. Draft International Standards adopted by the joint technical committee are circulated to national bodies for voting. Publication as an International Standard requires approval by at least 75 % of the national bodies casting a vote.

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.

ISO/IEC 30111 was prepared by Joint Technical Committee ISO/IEC JTC 1, *Information technology*, Subcommittee SC 27, *Security techniques*.

Introduction

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

The audience for this standard includes consumers, developers, vendors, and evaluators of secure IT products. The following audiences may use this standard:

— developers and vendors, when responding to reported actual or potential vulnerabilities;

— evaluators, when assessing the security assurance afforded by vendors' and developers' vulnerability handling processes and the associated products and services;

— consumers, when selecting product and online service vendors to express best practice assurance requirements to developers, vendors and integrators.

This International Standard is related to ISO/IEC 29147.[5] It interfaces with elements described in ISO/IEC 29147 at the point of receiving potential vulnerability reports, and at the point of distributing vulnerability resolution information.

This International Standard takes into consideration the relevant elements of ISO/IEC 15408-3,[1] 13.5 Flaw remediation (ALC_FLR).

Information technology — Security techniques — Vulnerability handling processes

1 Scope

This International Standard gives guidelines for how to process and resolve potential vulnerability information in a product or online service.

This International Standard is applicable to vendors involved in handling vulnerabilities.

2 Normative references

The following documents, in whole or in part, are normatively referenced in this document and are indispensable for its application. 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*

3 Terms and definitions

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

3.1
coordinator
optional participant that can assist vendors and finders in handling and disclosing vulnerability information

Note 1 to entry: Acts as trusted liaison between involved parties, enabling communication between involved parties (vendors and finders).

3.2
online service
service which is implemented by hardware, software or a combination of them, and provided over a communication line or network

EXAMPLE Search engines, online backup services, Internet-hosted email, and software as a service are considered to be online services.

3.3
product
system or service implemented or refined for sale or to be offered for free

Note 1 to entry: In information technology, a distinction is often made between hardware and software products, although the boundary is not always clear.

EXAMPLE A router can be seen as a hardware product even though a vital component of it is software and/or firmware.

3.4
remediation
patch, fix, upgrade, configuration or documentation change to address a vulnerability

Note 1 to entry: A change intended to resolve or mitigate a vulnerability. A remediation typically takes the form of a configuration change, binary file replacement, hardware change, or source code patch, etc. Remediations are usually provided by vendors. Vendors use different terms including update, patch, fix, hotfix, and upgrade.

3.5
service
means of delivering value to users by facilitating results users want to achieve without the ownership of specific resources and risks

3.6
system
combination of interacting elements organized to achieve one or more stated purposes

[SOURCE: ISO/IEC 15288:2008, 4.31]

3.7
vendor
person or organization that developed the product, or service, or is responsible for maintaining it

3.8
vulnerability
weakness of software, hardware, or online service that can be exploited

[SOURCE: ISO/IEC 27000:2009, 2.46, modified]

Note 1 to entry: Examples of weaknesses in a system are software and hardware design flaws, poor administrative processes, lack of awareness and education, and advancements in the state of the art or improvements to current practices. Regardless of cause, an exploitation of such vulnerabilities may result in real threats to mission-critical information systems.

4 Abbreviated terms

CSIRT Computer Security Incident Response Team

PSIRT Product Security Incident Response Team

5 Interface between ISO/IEC 29147 - Vulnerability disclosure and ISO/IEC 30111 - Vulnerability handling processes

ISO/IEC 29147[5] - Vulnerability disclosure and ISO/IEC 30111 - Vulnerability handling processes are related standards, as Figure 1 shows. ISO/IEC 29147 provides a guideline for vendors to include in their normal business processes on receiving information about potential vulnerabilities from people or organizations externally and distributing vulnerability resolution information to affected users. ISO/IEC 30111 gives guidelines for how to process and resolve potential vulnerability information reported by individuals or organizations that find a potential vulnerability in a product or online service. While ISO/IEC 29147 deals with the interface between vendors and those who find and report potential vulnerabilities, ISO/IEC 30111 deals with the investigation, triage, and resolution of vulnerabilities, regardless if the source of the potential vulnerability was external to the vendor, or from within the vendor's own organization, typically security, development, or testing teams.

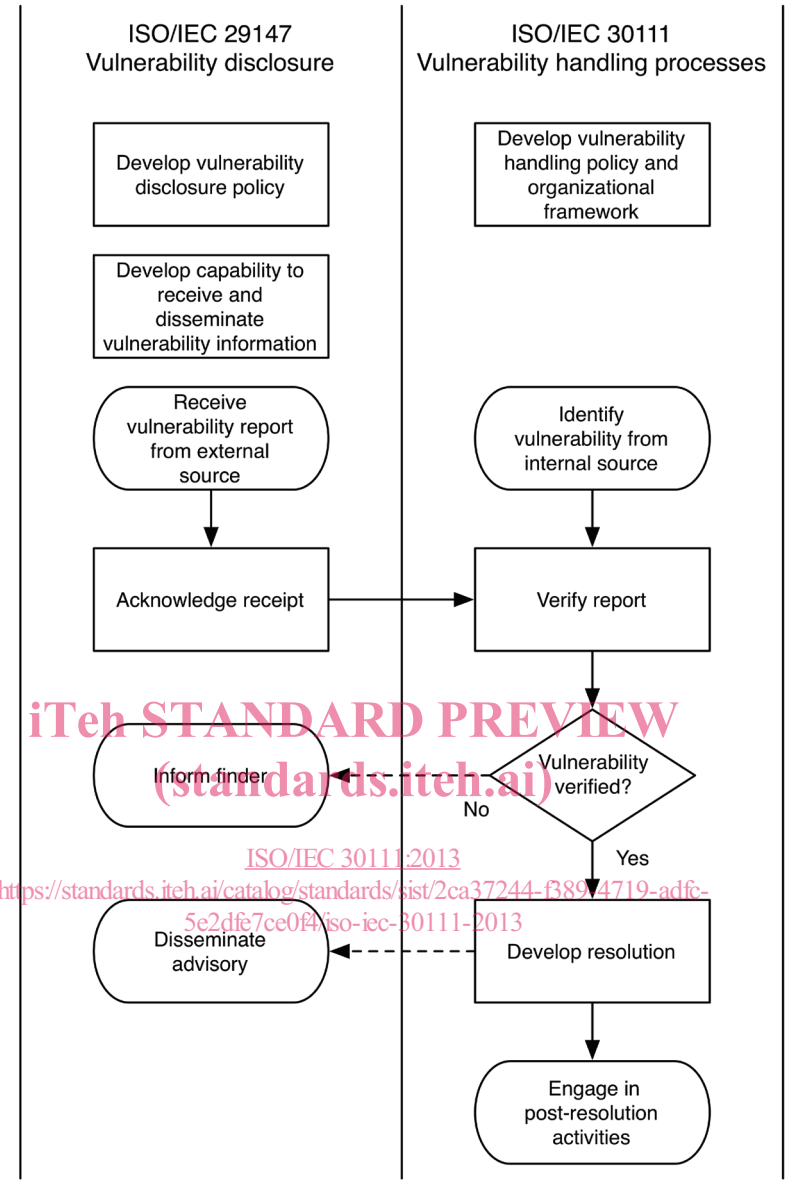

Figure 1 — A model of the Interface between ISO/IEC 29147 and ISO/IEC 30111

6 Policy and Organizational Framework for Vulnerability Handling Processes

6.1 General

Vendors should create a vulnerability handling process in accordance with this International Standard in order to prepare for investigating and resolving potential vulnerabilities. The creation of a vulnerability handling process is a task that is performed by a vendor, and should be periodically assessed to facilitate process improvement opportunities and ensure that the process performs as expected. Vendors should document their vulnerability handling procedure in order to ensure that it is repeatable. The documentation should describe the procedures and methods used to track all reported vulnerabilities.

See ISO/IEC 27034[3] for information on how identification of the root cause of a vulnerability, which is a step in the process of vulnerability handling, can help improve secure software development lifecycles and result in an outcome of more secure product development. The following clause describes the elements that vendors should consider included in their vulnerability handling processes.

6.2 Vulnerability Handling Policy Development

A vendor should develop and maintain a vulnerability handling policy to define and clarify its intentions when investigating and remediating vulnerabilities for the development of a vulnerability handling process. The policy should consist of two parts: an internal-only portion and a public portion.

The internal-only part of the policy is intended for the vendor's staff and defines who is responsible in each stage of the vulnerability handling process and how they should handle information on potential vulnerabilities. It should include the following items:

a) basic guidance, principles, and responsibilities for handling potential vulnerabilities in products or online services;

b) a list of departments and roles responsible for handling potential vulnerabilities;

c) safeguards to prevent premature disclosure of information about potential vulnerabilities before they are fixed.

The audience for the public part of the vulnerability handling policy is internal and external stakeholders, including finders who wish to report potential vulnerabilities, and users of the vendor's products or online services. It informs the audience of how the vendor is willing to interact with them when a potential vulnerability is found in the vendor's product or online services. Guidance, details and examples of public vulnerability handling policies are described in the sections describing vulnerability disclosure processes in ISO/IEC 29147.[5]

6.3 Development of an Organizational Framework to Support the Vulnerability Handling Process

6.3.1 General

Handling vulnerabilities has several additional aspects than just engineering and technology (for example, customer service and public relations). An organizational framework should be designed, recognized, and supported by the stakeholder divisions of the vendor responsible for each area.

An organization should have a role or capability that is responsible for and has authority to make decisions on vulnerability handling, preferably at a management level. This role or capability must understand the responsibility toward the vendor's users, the internal processes, and the organizational framework for vulnerability handling.

An organization should have a role or capability that is a point of contact for handling potential vulnerabilities. This point of contact should be identified for each division or department within a vendor that provides products or online services to customers.

An organization should establish a point of contact for external parties to reach and communicate with about vulnerabilities. The point of contact may be part of a vendor computer security incident response team (vendor CSIRT) or a product security incident response team (PSIRT). Its details are discussed in 6.4.

Since customers and members of the media may contact the vendor with questions or requests for additional information after a vulnerability is disclosed, divisions responsible for customer and public relations should be prepared so that they can respond.

6.4 Vendor CSIRT or PSIRT

6.4.1 General

A vendor CSIRT or PSIRT is responsible for coordinating vulnerability reports from external finders of vulnerabilities. In some cases, a vendor PSIRT also coordinates vulnerabilities that were reported by internal teams within the vendor. The following clauses describe the organizational role and responsibilities of a vendor CSIRT or PSIRT. For clarity, PSIRT will be used to refer to this role throughout the rest of the document.

6.4.2 Vulnerability Response Team Mission

In vendor's vulnerability handling process, a vendor PSIRT plays a central role. In addition to coordinating vulnerability handling internally, it acts as a single point of contact for outside stakeholders such as finders of vulnerability and coordinators.

The function of a vendor PSIRT should be implemented centrally within the vendor, though it can be implemented within a product business division, if there is only a single product business division providing major products or online services from the vendor.

6.4.3 Vulnerability Response Team Responsibilities

6.4.3.1 General

This clause describes the responsibilities of vulnerability response teams.

6.4.3.2 Communication with external finders of potential vulnerabilities

A vendor PSIRT should develop a single entry-point for receiving potential vulnerability reports from finders or coordinators, typically either an e-mail address or a form on a web page.

A vendor PSIRT is responsible for maintaining communication with finders who reported potential vulnerabilities. It is important for vendors to understand the importance of timeliness, and finders' different agenda and stances on vulnerabilities.

6.4.3.3 Communication with product business divisions

A vendor PSIRT shall work with product and online services divisions to build a database of contacts for each product. When a potential vulnerability is reported, the PSIRT shall identify the responsible product business division to dispatch the report to them through the contact person. The information shall be shared confidentially on a need-to-know basis.

6.4.3.4 Communication with coordinators or other vendors

Where appropriate, a vendor PSIRT shall make an arrangement for sharing vulnerability information with coordinators or other vendors. They should be conscious of the vulnerability handling policy of the other party.

6.4.3.5 Timing of vulnerability disclosure

A vendor PSIRT shall choose an appropriate date for each vulnerability disclosure and prepare the advisory with the assistance of the product business division and other major stakeholders, such as coordinators if applicable.

