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)

COPYRIGHT PROTECTED DOCUMENT

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.