INTERNATIONAL STANDARD

ISO/IEC 29147

First edition
2014-02-15

Information technology — Security techniques — Vulnerability disclosure

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

Reference number
ISO/IEC 29147:2014(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 29147 was prepared by Joint Technical Committee ISO/IEC JTC 1, *Information technology*, Subcommittee SC 27, *IT Security techniques*.

Introduction

A vulnerability is a weakness of software, hardware, or online service that can be exploited. An exploitation of vulnerabilities results in a disruption of the confidentiality, integrity, or availability of the ICT system or related information assets, which may cause a breach of data privacy, interruption of operation of mission critical systems, and so on.

Vulnerabilities can be caused by both software or hardware design and programming flaws. Poor administrative processes and a lack of user awareness and education can also be a source of vulnerabilities, as can unforeseen changes in operating environments. Regardless of the cause, an exploitation of such vulnerabilities may result in real threats to mission-critical information systems. Individuals and organizations, including businesses and governments, rely heavily on hardware and software components used in operating systems, applications, networks, and critical national infrastructure. Vulnerabilities in these components increase risk to the information residing on them, thus increasing risks to users and owners of the information. In addition, the lack of awareness about these vulnerabilities also increases risk.

Inappropriate disclosure of a vulnerability could not only delay the deployment of the vulnerability resolution but also give attackers hints to exploit it. That is why vulnerability disclosure should be carried out appropriately.

Vulnerability disclosure is a process through which vendors and vulnerability finders may work cooperatively in finding solutions that reduce the risks associated with a vulnerability. It encompasses actions such as reporting, coordinating, and publishing information about a vulnerability and its resolution.

The goals of vulnerability disclosure include the following:

a) ensuring that identified vulnerabilities are addressed;

b) minimizing the risk from vulnerabilities;

c) providing users with sufficient information to evaluate risks from vulnerabilities to their systems;

d) setting expectations to promote positive communication and coordination among involved parties.

This International Standard provides guidelines for vendors to be included in their business processes when receiving information about potential vulnerabilities and distributing vulnerability resolution information.

Information technology — Security techniques — Vulnerability disclosure

1 Scope

This International Standard gives guidelines for the disclosure of potential vulnerabilities in products and online services. This International Standard details the methods a vendor should use to address issues related to vulnerability disclosure. This International Standard

a) provides guidelines for vendors on how to receive information about potential vulnerabilities in their products or online services,

b) provides guidelines for vendors on how to disseminate resolution information about vulnerabilities in their products or online services,

c) provides the information items that should be produced through the implementation of a vendor's vulnerability disclosure process, and

d) provides examples of content that should be included in the information items.

This International Standard is applicable to vendors who respond to external reports of vulnerabilities in their products or online services.

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 27000:2012, *Information technology — Security techniques — Information security management systems — Overview and vocabulary*

ISO/IEC 30111, *Information technology — Security techniques — Vulnerability handling processes*

3 Terms and definitions

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

3.1
advisory
announcement or bulletin that serves to inform, advise, and warn about a vulnerability of a product

Note 1 to entry: An advisory may include advice on how to deal with the vulnerability. An advisory typically contains a description of the vulnerability at a specific point in time. An advisory can include a list of vulnerable products or services, potential impact, resolution and mitigation information, and references. Such items included in the advisory are relevant at the time the advisory is published and may evolve over time. An advisory may be published by a vendor, finder, or coordinator and may be revised if more information becomes available.

3.2
coordinator
optional participant that can assist vendors and finders in handling and disclosing vulnerability information

Note 1 to entry: A coordinator can act as a trusted liaison between involved parties (vendors and finders), enabling positive communication between them.