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.

3.3
finder
individual or organization that identifies a potential vulnerability in a product or online service

Note 1 to entry: Finders can be researchers, security companies, users, governments, or coordinators.

3.4
online services
service which is implemented by hardware, software, or a combination of them and provided over a communication line or network

Note 1 to entry: The vendor of an online service may also be referred to as a service provider. Online services are similar to products in that both are primarily software systems. Two main distinctions are that a service often appears to users as a single instance of software and that users do not install, manage, or deploy the software, but they only use the service.

3.5
product
system implemented or developed for sale or to be offered for free

3.6
remediation
patch, fix, upgrade, configuration, or documentation change to either remove or mitigate a vulnerability

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

Note 2 to entry: Actions that reduce the impact of a possible attack or mask the vulnerability (which are, in most cases, a temporary action) are often called countermeasures or workarounds.

3.7
service
means of delivering value to users by facilitating results users want to achieve without the ownership of specific physical or logical resources and the risks related to ownership

3.8
vendor
individual or organization that developed the product or service or is responsible for maintaining it

3.9
vulnerability
weakness of software, hardware, or online service that can be exploited

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

Note 1 to entry: Weaknesses in a system can be caused by 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.

4 Abbreviated terms

CCE	Common Configuration Enumeration
CPE	Common Platform Enumeration
CSIRT	Computer Security Incident Response Team
CVE	Common Vulnerabilities and Exposures
CVSS	Common Vulnerability Scoring System

ID	identifier
IT	information technology
PC	personal computer
PDF	portable document format
PGP	Pretty Good Privacy
PoC	proof of concept
PSIRT	product security incident response team
SRM	secure receiving model
SW	software
URL	uniform resource locator

5 Concepts

5.1 General

The purpose of this clause is to provide background information and context to help readers better understand vulnerability handling and vulnerability disclosure.

5.2 Interface between ISO/IEC 29147: Vulnerability disclosure and ISO/IEC 30111: Vulnerability handling processes

ISO/IEC 29147: Vulnerability disclosure and ISO/IEC 30111: Vulnerability handling processes are related standards, as Figure 1 shows.

ISO/IEC 29147 provides guidelines for vendors to include in their normal business processes when receiving information about potential vulnerabilities from external individuals or organizations and when distributing vulnerability resolution information to affected users. This targets individuals, persons, users, and organizations who require methods to receive vulnerability reports and, when required, to disseminate advisories.

ISO/IEC 30111 gives guidelines on how to process and resolve potential vulnerability information reported by individuals or organizations that find a potential vulnerability in a product or online service. This is targeted at organizations who want to strengthen their internal processing to deal with received vulnerability reports.

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 security, development, or testing teams.

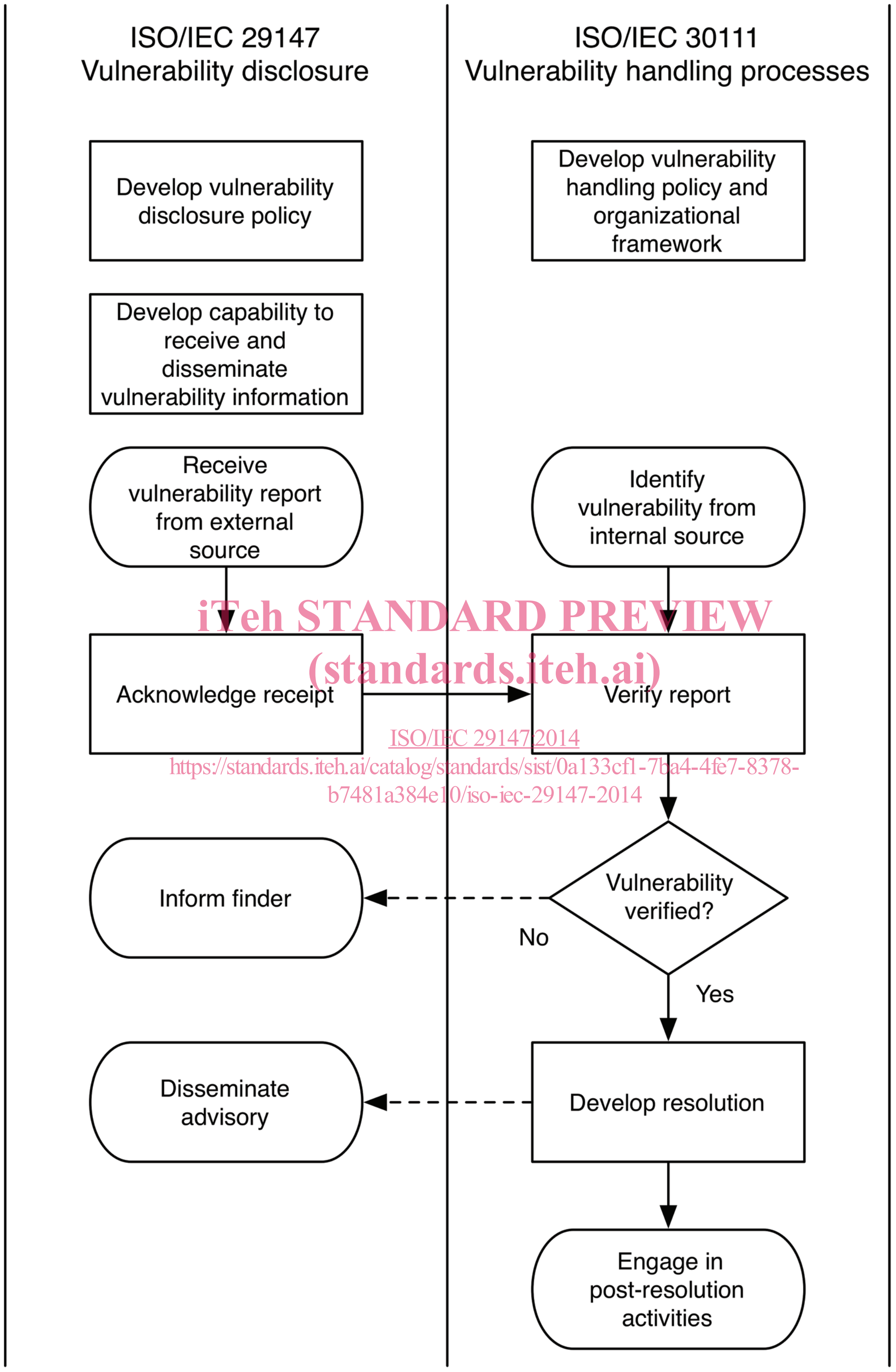
ISO/IEC 29147
Vulnerability disclosure
ISO/IEC 30111
Vulnerability handling processes
Develop vulnerability disclosure policy
Develop vulnerability handling policy and organizational framework
Develop capability to receive and disseminate vulnerability information
Receive vulnerability report from external source
Identify vulnerability from internal source
Acknowledge receipt
Verify report
Inform finder
Vulnerability verified?
No
Yes
Disseminate advisory
Develop resolution
Engage in post-resolution activities

Figure 1 — Mapping of ISO/IEC 29147 and ISO/IEC 30111

5.3 Products and online services

5.3.1 Products

Products are systems provided by vendors to users either for sale or for free. There are many different types of products including but not limited to custom software built under contract for specific user's license use, libraries intended to be included in other products, commercial off-the-shelf (COTS) products for mass markets, community-developed projects, and recreational or hobbyist offerings.

For the purposes of this International Standard, the distinction between hardware and software products is seldom relevant. There are very few cases of vulnerabilities in pure hardware systems. In most cases, so-called hardware vulnerabilities actually occur in low-level software or firmware.

Depending on sales, distribution, and support models, vendors may or may not have accurate lists of users. This can be relevant when considering notifying affected users of a vulnerability.

5.3.2 Vulnerability

A vulnerability is generally a set of conditions that allows the violation of an explicit or implicit security policy of the user. Typically, the violation of the user's security policy results in a negative impact or loss to the user. One common way to categorize loss is to consider the impact to the confidentiality, integrity, and availability of an asset. For example, a vulnerability that allowed an attacker to install malicious software on a user's system might severely impact confidentiality and integrity since the attacker could use the malicious software to read or change sensitive information. A vulnerability in a network product that caused the product to experience a system error would impact availability. The actual impact of a vulnerability depends on how the vulnerable product is used and other subjective factors.

Vulnerabilities are often caused by implementation defects in software. A vulnerability can be associated with the security policy if one exists. One common type of vulnerability includes buffer overflows and related low-level memory management errors that allow specially crafted input to control execution of the vulnerable software program. SQL injection and cross-site scripting vulnerabilities are common types of vulnerabilities found in web applications. Many other sets of conditions can cause or contribute to vulnerabilities, including design decisions, default configuration settings, weak authentication or access control, lack of awareness or education, or even unexpected interactions between systems or changes in operating environments.

More information about types of vulnerabilities can be found in the Common Weakness Enumeration (CWE) and the Open Web Application Security Project (OWASP). Both of these organizations focus on training developers and engineers on current security threats including how to discover and rate them and how to programmatically make code and applications better. Links to both of these sites are located in B.4.

Many stakeholders (predominantly vendors and users) seek to identify and resolve vulnerabilities, either removing them entirely (usually by patching or updating software to remove defects) or by mitigating or working around vulnerabilities to reduce the likelihood and/or impact of successful attack. Vulnerability disclosure provides vendors and users with information to resolve and mitigate vulnerabilities and to make better risk decisions.

Attackers also seek to identify vulnerabilities, but typically do not attempt to disclose or resolve vulnerabilities. Attackers seek to exploit vulnerabilities for some gain, almost always causing loss to users.

5.3.3 Product interdependency

Many products are complex systems that include other products in some way. Products can use source code from other products, software libraries, or other types of interfaces. Some products are substantially similar but sold under different brands by different vendors. Different products that support the same network protocol or file format may be affected by a vulnerability in the protocol or format. A user or vendor may not be certain which products are affected by the vulnerability. These interdependencies are important since products that use or interact with a vulnerable product may also be vulnerable.

5.4 Stakeholders

This subclause enumerates major stakeholders in the vulnerability disclosure process.

5.4.1 User

Users may directly operate software or hardware products or make use of an online service. Users may be referred to as consumers, customers, or end users. Due to the interdependencies of modern software products, users may not know precisely which components or products they are actually using.

Users need information about vulnerabilities, particularly remediation, in order to make effective risk decisions and to use software products and online services more securely. Providing vulnerability information to users is discussed in Clause 9.

5.4.2 Vendor

A vendor develops a product or online service or is responsible for maintaining it. A vendor may be an individual or organization such as a commercial business or an open source project. There are a number of different terms used to describe individuals or organizations who deliver software products for free, including developer, maintainer, or distributor. Similarly, an individual or organization that delivers software products within a supply chain may be called a supplier. For the purposes of this International Standard, the term “vendor” shall be used to mean all of them.

Vendors are responsible for the quality of their products and online services. Vendors use vulnerability disclosure to learn about vulnerabilities, to develop resolutions and mitigations, and to distribute information to users.

There are many types of vendors with various models for developing, selling, supporting, and distributing products. Some vendors integrate products into a system or service, and these vendors may act as customers or users of the component products. These intermediate vendors may be dependent on component vendors for vulnerability resolution and mitigation information.

5.4.3 Intermediate Vendor

An intermediate vendor gets a subsystem from a vendor and uses it to supply a system or service (or a combination of both) to a user (or another intermediate vendor). Typical examples are the following:

a) system houses that use a PC and an operating system to add their own healthcare administration software and sell the combined system to a medical doctor (maybe together with a maintenance contract);

b) telecommunication providers that supply a mobile phone together with a service contract.

These intermediate vendors may learn about vulnerabilities through error reports from their customers and additional early investigations (e.g. as part of quality controls for incoming goods). They shall report vulnerabilities to their vendors. The difficult issue for intermediate vendors is that they may not be in a position to simply wait for their vendor to solve the problem and remove the vulnerability.

They have a legal responsibility to inform their customers, as the customers may need to stop using the device or some of its functionality or to work around the vulnerabilities in order to mitigate risk. This holds especially when the vendor takes a long time to remove the vulnerability or is not able to do so at all. If an intermediate vendor informs its customer, this may well mean that vulnerability is disclosed before the vendor is able to deal with this.

Intermediate vendors may also be technically capable of producing and distributing workarounds to at least protect the use of their product or service or even a specific configuration of the underlying system (e.g. a more restrictive configuration of the operating system). Their intermediary role puts these vendors in the position of having to deal with trade-offs (e.g. informing their customers about vulnerabilities quickly vs. communicating solutions in addition to problems).

5.4.4 Finder

A finder is an individual or organization who identifies a potential vulnerability in a product or an online service. A finder is often a security or vulnerability researcher. A finder may also be a user or vendor. For the purposes of this International Standard, it is expected that a finder will attempt to inform a vendor or coordinator about a vulnerability. In practice, a finder may choose not to attempt to inform a vendor or coordinator or the attempt may fail. Receiving vulnerability information from finders is discussed in Clause 7.

5.4.5 Coordinator

Coordinators may work with other coordinators to obtain help with domain expertise, language, time zone, and cultural barriers and to share effort. Some Computer Security Incident Response Teams (CSIRTs) provide vulnerability coordination services on an operational basis, and other CSIRTs will help coordinate individual cases. Some vendors also provide coordination services.

Common services provided by a coordinator include

— helping finders identify and contact vendors,

— coordinating vulnerabilities that affect multiple vendors,

— performing technical analysis and validation of vulnerability reports, and

— publishing advisories.

While coordinators often have interests in protecting their constituencies, coordinators should attempt to be technically objective and minimize risk to all stakeholders.

5.5 Vulnerability disclosure process summary

This subclause summarizes the vulnerability disclosure process contained in ISO/IEC 30111. Figure 2 outlines the vendor's vulnerability disclosure process which consists of the five high-level steps.

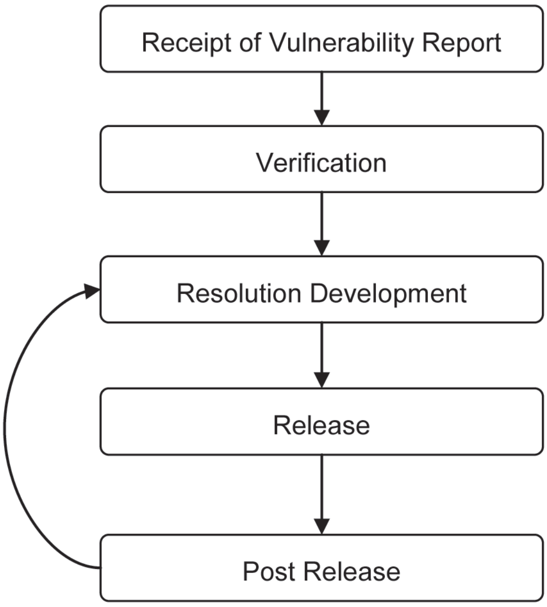

Figure 2 — Summary vulnerability disclosure process