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*

iTeh STANDARD PREVIEW

ISO/IEC 29147:2014

b7481a384e10/iso-iec-29147-2014

Reference number
ISO/IEC 29147:2014(E)

© ISO/IEC 2014

iTeh STANDARD PREVIEW

ISO/IEC 29147:2014

b7481a384e10/iso-iec-29147-2014



COPYRIGHT PROTECTED DOCUMENT

# Contents

Page

**Foreword** ... **iv**

**Introduction** ... **v**

**1 Scope** ... **1**

**2 Normative references** ... **1**

**3 Terms and definitions** ... **1**

**4 Abbreviated terms** ... **2**

**5 Concepts** ... **3**
5.1 General ... 3
5.2 Interface between ISO/IEC 29147: Vulnerability disclosure and ISO/IEC 30111: Vulnerability handling processes ... 3
5.3 Products and online services ... 5
5.4 Stakeholders ... 6
5.5 Vulnerability disclosure process summary ... 7
5.6 Information exchange during vulnerability disclosure ... 8
5.7 Confidentiality of exchanged information ... 9
5.8 Vulnerability advisories ... 9
5.9 Vulnerability exploitation ... 9

**6 Vulnerability disclosure policy considerations** ... **10**
6.1 General ... 10
... 10
... 11

... **12**
... 12
... 12
... 12
... 12
... 12
... 12
... 13

... **13**
... 13
... 13
... 13

... **14**
... 14
... 14
... 14
... 14
... 15
... 16
... 17
... 17

**ation** ... **18**

**rs** ... **26**

... **34**

iTeh STANDARD PREVIEW

# 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*.

iTeh STANDARD PREVIEW

# 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.

iTeh STANDARD PREVIEW

rabilities to their systems;

on among involved parties.

n their business processes
g vulnerability resolution

iTeh STANDARD PREVIEW

ISO/IEC 29147:2014

b7481a384e10/iso-iec-29147-2014

# 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

iTeh STANDARD PREVIEW

in this document and are
ited applies. For undated
ndments) applies..

*ation security management*

*handling processes*

0 and the following apply.

lnerability of a product

ability. An advisory typically
an include a list of vulnerable
ferences. Such items included
ver time. An advisory may be
n becomes available.

d disclosing vulnerability

endors and finders), enabling

**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.

iTeh STANDARD PREVIEW

Note 2 to entry: Actions that
cases, a temporary action) ar

**3.7**
**service**
means of delivering value t
specific physical or logical

**3.8**
**vendor**
individual or organization

**3.9**
**vulnerability**
weakness of software, har

[SOURCE: ISO/IEC 27000:2

Note 1 to entry: Weaknesses i
processes, lack of awareness
practices.

## 4 Abbreviated term

CCE Common Configu

CPE Common Platfor

CSIRT Computer Securi

CVE Common Vulnera

CVSS Common Vulnera

| | |
|---|---|
| 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

iTeh STANDARD PREVIEW

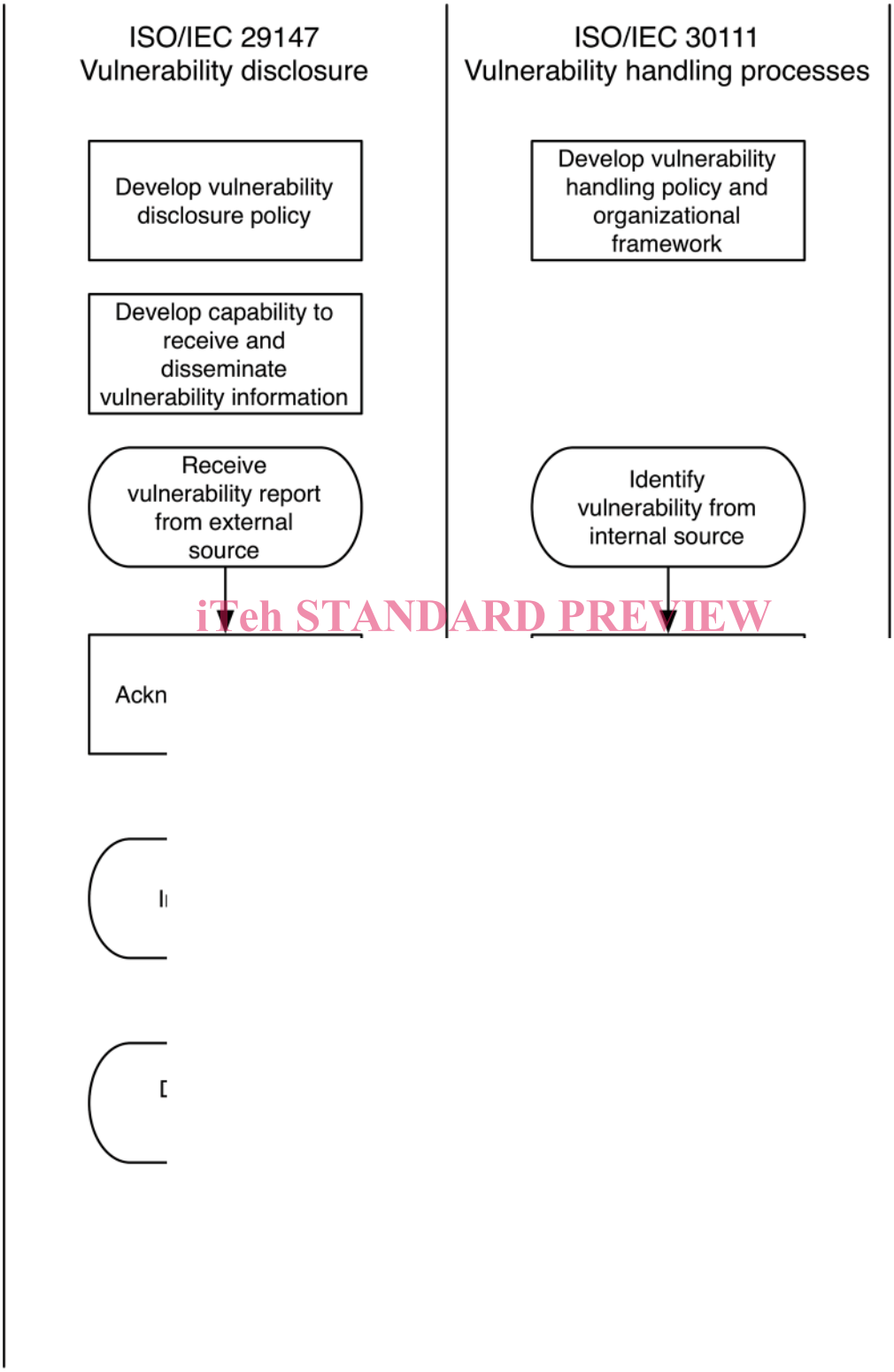
**d ISO/IEC 30111: Vul-**

dling processes are related

business processes when
uals or organizations and
. This targets individuals,
ability reports and, when

vulnerability information
a product or online service.
ssing to deal with received

o find and report potential
solution of vulnerabilities,
vendor or from within the




iTeh STANDARD PREVIEW

**Figu**

## 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

iTeh STANDARD PREVIEW

ctive factors.

erability can be associated
ludes buffer overflows and
input to control execution
ulnerabilities are common
ns can cause or contribute
s, weak authentication or
tions between systems or

on Weakness Enumeration
ese organizations focus on
to discover and rate them
th of these sites are located

nd resolve vulnerabilities,
to remove defects) or by
d/or impact of successful
on to resolve and mitigate

pt to disclose or resolve
ost always causing loss to

y. Products can use source
products are substantially
ucts that support the same
otocol 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.

iTeh STANDARD PREVIEW

Vendors are responsible fo
disclosure to learn about
information to users.

There are many types o
distributing products. Som
act as customers or users
component vendors for vu

### 5.4.3 Intermediate Ven

An intermediate vendor g
a combination of both) to a

a) system houses that us
software and sell the
contract);

b) telecommunication pr

These intermediate vendo
and additional early invest
vulnerabilities to their ven
position to simply wait for

They have a legal responsi
device or some of its funct
holds especially when the
all. If an intermediate ven
before the vendor is able t

Intermediate vendors ma
at least protect the use of
system (e.g. a more restri

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

iTeh STANDARD PREVIEW

ordinators should attempt

in ISO/IEC 30111. Figure 2
ive high-level steps.

**cess**