BS EN ISO/IEC 29147:2020

BSI Standards Publication

Information technology – Security techniques – Vulnerability disclosure

Documents
Document Sharing Hub

Full document details: BS EN ISO/IEC 29147:2020

National foreword

This British Standard is the UK implementation of EN ISO/IEC 29147:2020. It is identical to ISO/IEC 29147:2018. It supersedes BS ISO/IEC 29147:2018, which is withdrawn.

The UK participation in its preparation was entrusted to Technical Committee IST/33, Information security, cybersecurity and privacy protection.

A list of organizations represented on this committee can be obtained on request to its secretary.

This publication does not purport to include all the necessary provisions of a contract. Users are responsible for its correct application.

© The British Standards Institution 2020
Published by BSI Standards Limited 2020

ISBN 978 0 539 06990 7

ICS 35.030

Compliance with a British Standard cannot confer immunity from legal obligations.

This British Standard was published under the authority of the Standards Policy and Strategy Committee on 31 October 2018.

Amendments/corrigenda issued since publication

Date	Text affected
30 June 2020	This corrigendum renumbers BS ISO/IEC 29147:2018 as BS EN ISO/IEC 29147:2020

Documents
Document Sharing Hub

Full document details: BS EN ISO/IEC 29147:2020

EUROPEAN STANDARD

NORME EUROPÉENNE

EUROPÄISCHE NORM

EN ISO/IEC 29147

May 2020

ICS 35.030

English version

Information technology - Security techniques - Vulnerability disclosure (ISO/IEC 29147:2018)

Technologies de l'information - Techniques de sécurité - Divulgation de vulnérabilité (ISO/IEC 29147:2018)

Informationstechnik - Sicherheitstechniken - Offenlegung von Schwachstellen (ISO/IEC 29147:2018)

This European Standard was approved by CEN on 3 May 2020.

CEN and CENELEC members are bound to comply with the CEN/CENELEC Internal Regulations which stipulate the conditions for giving this European Standard the status of a national standard without any alteration. Up-to-date lists and bibliographical references concerning such national standards may be obtained on application to the CEN-CENELEC Management Centre or to any CEN and CENELEC member.

This European Standard exists in three official versions (English, French, German). A version in any other language made by translation under the responsibility of a CEN and CENELEC member into its own language and notified to the CEN-CENELEC Management Centre has the same status as the official versions.

CEN and CENELEC members are the national standards bodies and national electrotechnical committees of Austria, Belgium, Bulgaria, Croatia, Cyprus, Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Iceland, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, Netherlands, Norway, Poland, Portugal, Republic of North Macedonia, Romania, Serbia, Slovakia, Slovenia, Spain, Sweden, Switzerland, Turkey and United Kingdom.

CEN-CENELEC Management Centre:
Rue de la Science 23, B-1040 Brussels

© 2020 CEN/CENELEC All rights of exploitation in any form and by any means reserved worldwide for CEN national Members and for CENELEC Members.

Ref. No. EN ISO/IEC 29147:2020 E

AVA Documents
Document Sharing Hub

Full document details: BS EN ISO/IEC 29147:2020

European foreword

The text of ISO/IEC 29147:2018 has been prepared by Technical Committee ISO/IEC JTC 1 "Information technology" of the International Organization for Standardization (ISO) and has been taken over as EN ISO/IEC 29147:2020 by Technical Committee CEN/CLC/JTC 13 "Cybersecurity and Data Protection" the secretariat of which is held by DIN.

This European Standard shall be given the status of a national standard, either by publication of an identical text or by endorsement, at the latest by November 2020, and conflicting national standards shall be withdrawn at the latest by November 2020.

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights. CEN shall not be held responsible for identifying any or all such patent rights.

According to the CEN-CENELEC Internal Regulations, the national standards organizations of the following countries are bound to implement this European Standard: Austria, Belgium, Bulgaria, Croatia, Cyprus, Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Iceland, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, Netherlands, Norway, Poland, Portugal, Republic of North Macedonia, Romania, Serbia, Slovakia, Slovenia, Spain, Sweden, Switzerland, Turkey and the United Kingdom.

Endorsement notice

The text of ISO/IEC 29147:2018 has been approved by CEN as EN ISO/IEC 29147:2020 without any modification.

Documents
Document Sharing Hub

Full document details: BS EN ISO/IEC 29147:2020

Contents

Page

Foreword ... **vi**
Introduction ... **vii**
1 Scope ... **1**
2 Normative references ... **1**
3 Terms and definitions ... **1**
4 Abbreviated terms ... **3**
5 Concepts ... **3**
5.1 General ... 3
5.2 Structure of this document ... 3
5.3 Relationships to other International Standards ... 4
5.3.1 ISO/IEC 30111 ... 4
5.3.2 ISO/IEC 27002 ... 5
5.3.3 ISO/IEC 27034 series ... 6
5.3.4 ISO/IEC 27036-3 ... 6
5.3.5 ISO/IEC 27017 ... 6
5.3.6 ISO/IEC 27035 series ... 6
5.3.7 Security evaluation, testing and specification ... 6
5.4 Systems, components, and services ... 6
5.4.1 Systems ... 6
5.4.2 Components ... 6
5.4.3 Products ... 6
5.4.4 Services ... 7
5.4.5 Vulnerability ... 7
5.4.6 Product interdependency ... 7
5.5 Stakeholder roles ... 8
5.5.1 General ... 8
5.5.2 User ... 8
5.5.3 Vendor ... 8
5.5.4 Reporter ... 8
5.5.5 Coordinator ... 9
5.6 Vulnerability handling process summary ... 9
5.6.1 General ... 9
5.6.2 Preparation ... 10
5.6.3 Receipt ... 10
5.6.4 Verification ... 11
5.6.5 Remediation development ... 11
5.6.6 Release ... 11
5.6.7 Post-release ... 12
5.6.8 Embargo period ... 12
5.7 Information exchange during vulnerability disclosure ... 12
5.8 Confidentiality of exchanged information ... 13
5.8.1 General ... 13
5.8.2 Secure communications ... 13
5.9 Vulnerability advisories ... 13
5.10 Vulnerability exploitation ... 14
5.11 Vulnerabilities and risk ... 14
6 Receiving vulnerability reports ... **14**
6.1 General ... 14
6.2 Vulnerability reports ... 14
6.2.1 General ... 14
6.2.2 Capability to receive reports ... 14
6.2.3 Monitoring ... 15

© ISO/IEC 2018 – All rights reserved

AVA Documents
Document Sharing Hub
Full document details: BS EN ISO/IEC 29147:2020

6.2.4 Report tracking ... 15
6.2.5 Report acknowledgement ... 15
6.3 Initial assessment ... 16
6.4 Further investigation ... 16
6.5 On-going communication ... 16
6.6 Coordinator involvement ... 16
6.7 Operational security ... 17

7 Publishing vulnerability advisories ... 17
7.1 General ... 17
7.2 Advisory ... 17
7.3 Advisory publication timing ... 17
7.4 Advisory elements ... 18
7.4.1 General ... 18
7.4.2 Identifiers ... 18
7.4.3 Date and time ... 18
7.4.4 Title ... 19
7.4.5 Overview ... 19
7.4.6 Affected products ... 19
7.4.7 Intended audience ... 19
7.4.8 Localization ... 19
7.4.9 Description ... 19
7.4.10 Impact ... 19
7.4.11 Severity ... 20
7.4.12 Remediation ... 20
7.4.13 References ... 20
7.4.14 Credit ... 20
7.4.15 Contact information ... 20
7.4.16 Revision history ... 20
7.4.17 Terms of use ... 20
7.5 Advisory communication ... 20
7.6 Advisory format ... 21
7.7 Advisory authenticity ... 21
7.8 Remediations ... 21
7.8.1 General ... 21
7.8.2 Remediation authenticity ... 21
7.8.3 Remediation deployment ... 21

8 Coordination ... 21
8.1 General ... 21
8.2 Vendors playing multiple roles ... 22
8.2.1 General ... 22
8.2.2 Vulnerability reporting among vendors ... 22
8.2.3 Reporting vulnerability information to other vendors ... 22

9 Vulnerability disclosure policy ... 22
9.1 General ... 22
9.2 Required policy elements ... 23
9.2.1 General ... 23
9.2.2 Preferred contact mechanism ... 23
9.3 Recommended policy elements ... 23
9.3.1 General ... 23
9.3.2 Vulnerability report contents ... 23
9.3.3 Secure communication options ... 24
9.3.4 Setting communication expectations ... 24
9.3.5 Scope ... 24
9.3.6 Publication ... 24
9.3.7 Recognition ... 24
9.4 Optional policy elements ... 24
9.4.1 General ... 24

© ISO/IEC 2018 – All rights reserved
Documents
Document Sharing Hub
Full document details: BS EN ISO/IEC 29147:2020

9.4.2 Legal considerations ... 24
9.4.3 Disclosure timeline ... 24

Annex A (informative) **Example vulnerability disclosure policies** ... **25**

Annex B (informative) **Information to request in a report** ... **26**

Annex C (informative) **Example advisories** ... **27**

Annex D (informative) **Summary of normative elements** ... **30**

Bibliography ... **32**

© ISO/IEC 2018 – All rights reserved

Documents
Document Sharing Hub

Full document details: BS EN ISO/IEC 29147:2020

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.

The procedures used to develop this document and those intended for its further maintenance are described in the ISO/IEC Directives, Part 1. In particular, the different approval criteria needed for the different types of document should be noted. This document was drafted in accordance with the editorial rules of the ISO/IEC Directives, Part 2 (see www.iso.org/directives).

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. Details of any patent rights identified during the development of the document will be in the Introduction and/or on the ISO list of patent declarations received (see www.iso.org/patents) or the IEC list of patent declarations received (see http://patents.iec.ch).

Any trade name used in this document is information given for the convenience of users and does not constitute an endorsement.

For an explanation of the voluntary nature of standards, the meaning of ISO specific terms and expressions related to conformity assessment, as well as information about ISO's adherence to the World Trade Organization (WTO) principles in the Technical Barriers to Trade (TBT) see www.iso.org/iso/foreword.html.

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

This second edition cancels and replaces the first edition (ISO/IEC 29147:2014), which has been technically revised.

The main changes compared to the previous edition are as follows:

— a number of normative provisions have been added (summarized in Annex D);

— numerous organizational and editorial changes have been made for clarity.

Any feedback or questions on this document should be directed to the user's national standards body. A complete listing of these bodies can be found at www.iso.org/members.html.

This document is intended to be used with ISO/IEC 30111.

© ISO/IEC 2018 – All rights reserved
Documents
Document Sharing Hub
Full document details: BS EN ISO/IEC 29147:2020

Introduction

In the contexts of information technology and cybersecurity, a vulnerability is a behaviour or set of conditions present in a system, product, component, or service that violates an implicit or explicit security policy. A vulnerability can be thought of as a weakness or exposure that allows a security impact or consequence. Attackers exploit vulnerabilities to compromise confidentiality, integrity, availability, operation, or some other security property.

Vulnerabilities often result from failures of a program or system to securely handle untrusted or unexpected input. Causes that lead to vulnerabilities include errors in coding or configuration, oversights in design choices, and insecure protocol and format specifications.

Despite significant efforts to improve software security, modern software and systems are so complex that it is impractical to produce them without vulnerabilities. Risk factors of vulnerabilities include:

— operating and relying on systems that have known vulnerabilities;

— not having sufficient information about vulnerabilities;

— not knowing that vulnerabilities exist.

This document describes vulnerability disclosure: techniques and policies for vendors to receive vulnerability reports and publish remediation information. Vulnerability disclosure enables both the remediation of vulnerabilities and better-informed risk decisions. Vulnerability disclosure is a critical element of the support, maintenance, and operation of any product or service that is exposed to active threats. This includes practically any product or service that uses open networks such as the Internet. A vulnerability disclosure capability is an essential part of the development, acquisition, operation, and support of all products and services. Operating without vulnerability disclosure capability puts users at increased risk.

The term “vulnerability disclosure” is used to describe the overall activities associated with receiving vulnerability reports and providing remediation information. Additional activities such as investigating and prioritizing reports, developing, testing, and deploying remediations, and improving secure development are called “vulnerability handling” and are described in ISO/IEC 30111. The term “disclosure” is also used more narrowly to mean the act of informing a party about a vulnerability for the first time (see 3.2).

Major goals of vulnerability disclosure include:

— reducing risk by remediating vulnerabilities and informing users;

— minimizing harm and cost associated with the disclosure;

— providing users with sufficient information to evaluate risk due to vulnerabilities;

— setting expectations to facilitate cooperative interaction and coordination among stakeholders.

The processes described in this document aim to minimize risk, cost, and harm to all stakeholders. Due to the volume of reported vulnerabilities, lack of accurate and complete information, and other factors involved, it is not possible to create a single, fixed process that applies to every disclosure event.

The normative elements in this document provide minimum requirements to create a functional vulnerability disclosure capability. Vendors should adapt the additional informative guidance in this document to fit their particular needs and those of users and other stakeholders.

© ISO/IEC 2018 – All rights reserved

Documents
Document Sharing Hub
Full document details: BS EN ISO/IEC 29147:2020

Documents
Document Sharing Hub

Full document details: BS EN ISO/IEC 29147:2020

Information technology — Security techniques — Vulnerability disclosure

1 Scope

This document provides requirements and recommendations to vendors on the disclosure of vulnerabilities in products and services. Vulnerability disclosure enables users to perform technical vulnerability management as specified in ISO/IEC 27002:2013, 12.6.1[1]. Vulnerability disclosure helps users protect their systems and data, prioritize defensive investments, and better assess risk. The goal of vulnerability disclosure is to reduce the risk associated with exploiting vulnerabilities. Coordinated vulnerability disclosure is especially important when multiple vendors are affected. This document provides:

— guidelines on receiving reports about potential vulnerabilities;

— guidelines on disclosing vulnerability remediation information;

— terms and definitions that are specific to vulnerability disclosure;

— an overview of vulnerability disclosure concepts;

— techniques and policy considerations for vulnerability disclosure;

— examples of techniques, policies (Annex A), and communications (Annex B).

Other related activities that take place between receiving and disclosing vulnerability reports are described in ISO/IEC 30111.

This document is applicable to vendors who choose to practice vulnerability disclosure to reduce risk to users of vendors' products and services.

2 Normative references

The following documents are referred to in the text in such a way that some or all of their content constitutes requirements of this document. 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*

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

3 Terms and definitions

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

ISO and IEC maintain terminological databases for use in standardization at the following addresses:

— ISO Online browsing platform: available at https://www.iso.org/obp

— IEC Electropedia: available at http://www.electropedia.org/

© ISO/IEC 2018 – All rights reserved

Documents
Document Sharing Hub
Full document details: BS EN ISO/IEC 29147:2020

3.1
vulnerability
functional behaviour of a product or service that violates an implicit or explicit security policy

Note 1 to entry: ISO/IEC 27002:2013, 12.6.1[1] uses the term "technical vulnerability" to distinguish between the more general risk-based concept of vulnerability and the term used in this document.

3.2
disclosure
act of initially providing *vulnerability* (3.1) information to a party that was not believed to be previously aware

3.3
coordination
set of activities including identifying and engaging stakeholders, mediating, communicating, and other planning in support of *vulnerability* (3.1) *disclosure* (3.2)

Note 1 to entry: The term "coordinated vulnerability disclosure" is used to denote a disclosure process that includes coordination.

3.4
vendor
individual or organization that is responsible for remediating vulnerabilities

Note 1 to entry: A vendor can be the developer, maintainer, producer, manufacturer, supplier, installer, or provider of a product or service.

3.5
reporter
individual or organization that notifies a *vendor* (3.4) or *coordinator* (3.6) of a potential *vulnerability* (3.1)

Note 1 to entry: There are no special requirements for acting as a reporter. Reporters can be individuals, organizations, amateurs or hobbyists, professionals, end-users, security research organizations, vendors, governments, or coordinators.

Note 2 to entry: The term "reporter" does not imply unique or original discovery or reporting.

Note 3 to entry: Reporters can be called researchers, whether or not the reporter explicitly performs security or vulnerability research. Historically, this role is also referred to as "finder."

3.6
coordinator
individual or organization that performs *coordination* (3.3)

3.7
remediation
change made to a product or service to remove or mitigate a *vulnerability* (3.1)

Note 1 to entry: A remediation typically takes the form of a binary file replacement, configuration change, or source code patch and recompile. Different terms used for "remediation" include patch, fix, update, hotfix, and upgrade. Mitigations are also called workarounds or countermeasures.

3.8
advisory
document or message that provides *vulnerability* (3.1) information intended to reduce risk

Note 1 to entry: An advisory is meant to inform users or other stakeholders about a vulnerability including, if possible, how to identify and remediate vulnerable systems.

© ISO/IEC 2018 – All rights reserved
Documents
Document Sharing Hub
Full document details: BS EN ISO/IEC 29147:2020

4 Abbreviated terms

COTS	common off-the-shelf
CRM	customer relationship management
CSIRT	computer security incident response team
CVE	common vulnerabilities and exposures[9]
CVRF	common vulnerability reporting format[12][13]
CVSS	common vulnerability scoring system[10]
CWE	common weakness enumeration[11]
HTTP(S)	hypertext transfer protocol (secure)
ICT	information and communication technology
OpenPGP	open pretty good privacy
OWASP	open web application security project
PoC	proof of concept
PSIRT	product security incident response team
S/MIME	secure multipurpose internet mail extensions
SQL	structured query language
TLS	transport layer security

5 Concepts

5.1 General

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

Vulnerability disclosure involves different stakeholders with different perspectives, incentives, capabilities, and available information. Furthermore, communication and process synchronization among multiple stakeholders can quickly become complicated. In practice, disclosure can deviate from the activities described in this document due to a variety of unforeseen circumstances.

5.2 Structure of this document

This document is meant to be read in its entirety as input to the development or improvement of vulnerability disclosure policies and processes. The remaining clauses of this document are organized as follows:

— Clause 5: Concepts;

— Clause 6: Receiving vulnerability reports;

— Clause 7: Publishing vulnerability advisories;

— Clause 8: Coordination;

© ISO/IEC 2018 – All rights reserved

Documents
Document Sharing Hub
Full document details: BS EN ISO/IEC 29147:2020

— Clause 9: Vulnerability disclosure policy.

The structure of this document is not meant to be followed in strict sequence as it appears above. For example, a vendor should ideally develop policy (Clause 9) before starting to receive reports (Clause 6).

Annex D contains a summary of all of the normative elements in this document.

5.3 Relationships to other International Standards

5.3.1 ISO/IEC 30111

ISO/IEC 30111 shall be used in conjunction with this document. The relationship between the two International Standards is illustrated in Figure 1.

This document provides guidelines for vendors to include in their normal business processes when receiving reports about potential vulnerabilities from external individuals or organizations and when distributing vulnerability remediation information to affected users.

ISO/IEC 30111 gives guidelines on how to investigate, process, and resolve potential vulnerability reports.

While this document deals with the interface between vendors and reporters, ISO/IEC 30111 deals with internal vendor processes including the triage, investigation, and remediation of vulnerabilities, whether the source of the report is external to the vendor or from within the vendor's own security, development, or testing teams.

© ISO/IEC 2018 – All rights reserved
Documents
Document Sharing Hub
Full document details: BS EN ISO/IEC 29147:2020