INTERNATIONAL STANDARD

ISO/IEC 29147

Second edition
2018-10

Information technology — Security techniques — Vulnerability disclosure

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

Reference number
ISO/IEC 29147:2018(E)

COPYRIGHT PROTECTED DOCUMENT

ISO copyright office
CP 401 • Ch. de Blandonnet 8
CH-1214 Vernier, Geneva
Phone: +41 22 749 01 11
Fax: +41 22 749 09 47
Email: copyright@iso.org
Website: 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.

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.

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.

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/

国际标准

ISO/IEC
29147

2018 年 10 月 第
二版

=

信息技术 - 安全技术 - 漏洞披露

信息技术 - 安全技术 - 漏洞披露

奥邦检验认证集团有限公司翻译
内部资料

Reference number ISO/IEC
29147:2018(E)

目录

前言

国际标准化组织（ISO）和国际电工委员会（IEC）构成了全球标准化的专业体系。作为 ISO 或 IEC 成员的各国机构通过各自组织为处理特定技术领域而设立的技术委员会参与国际标准的制定。ISO 和 IEC 的技术委员会在共同感兴趣的领域开展合作。其他国际组织，无论是政府的还是非政府的，通过与 ISO 和 IEC 的联络也参与相关工作。

本文件的编制程序以及其后续维护所采用的程序在 ISO/IEC 指令第 1 部分中有描述。尤其应注意不同类型的文件所需的不同批准标准。本文件是依照 ISO/IEC 指令第 2 部分的编辑规则起草的（见 www.iso.org/directives）。

请注意，本文件中的某些内容可能受专利权保护。国际标准化组织（ISO）和国际电工委员会（IEC）不对识别出的任何专利权负责。在文件编制过程中所识别出的专利权详情将在引言部分和/或国际标准化组织收到的专利声明清单（见 www.iso.org/patents）或国际电工委员会收到的专利声明清单（见 http://patents.iec.ch）中列出。

本文件中使用的任何商标名称均为方便用户而提供，不构成任何背书。

有关标准的自愿性、与合格评定相关的 ISO 专用术语和表达的含义，以及 ISO 遵守世界贸易组织（WTO）技术性贸易壁垒（TBT）原则的信息，请访问 www.iso.org/iso/foreword.html。

本文件由国际标准化组织/国际电工委员会联合技术委员会 ISO/IEC JTC 1（信息技术）下属的第 27 分技术委员会（安全技术）编制。

本第二版废止并取代了第一版（ISO/IEC 29147:2014），并对其进行了技术修订。

与上一版相比，主要的变化如下:

— 已增加了一些规范性条款（详见附件 D）；

— 为了清晰明了，已对组织结构和编辑内容做了大量修改。

关于本文件的任何反馈或疑问应提交给用户所在国家的标准机构。这些机构的完整列表可在 www.iso.org/members.html 查看。

本文件旨在与 ISO/IEC 30111 配合使用。

引言

在信息技术和网络安全领域，漏洞是指系统、产品、组件或服务中存在的违反隐含或明确安全策略的行为或一组条件。漏洞可以被视为一种弱点或暴露，它允许产生安全影响或后果。攻击者利用漏洞来破坏机密性、完整性、可用性、运行或其他安全属性。

漏洞通常是由程序或系统未能安全处理不受信任或意外的输入所导致的。导致漏洞的原因包括编码或配置错误、设计选择中的疏忽以及不安全的协议和格式规范。

尽管为提高软件安全性付出了巨大努力，但现代软件和系统极其复杂，以至于在没有漏洞的情况下开发它们是不切实际的。漏洞的风险因素包括：

— 运行和依赖存在已知漏洞的系统；

— 对漏洞缺乏足够的了解；

— 不知道存在漏洞。

本文件阐述了漏洞披露：供应商接收漏洞报告及发布补救信息的技术和政策。漏洞披露既有助于漏洞的修复，也有助于做出更明智的风险决策。漏洞披露是任何面临活跃威胁的产品或服务的支持、维护和运营的关键要素。这几乎涵盖了所有使用开放网络（如互联网）的产品或服务。漏洞披露能力是所有产品和服务开发、采购、运营和维护的重要组成部分。缺乏漏洞披露能力会增加用户面临的风险。

“漏洞披露”这一术语用于描述与接收漏洞报告以及提供补救信息相关的所有活动。诸如调查和优先处理报告、开发、测试和部署补救措施以及改进安全开发等其他活动被称为“漏洞处理”，这些内容在 ISO/IEC 30111 中有描述。“披露”一词有时也更狭义地指首次向某方告知漏洞的行为（见 3.2）。

漏洞披露的主要目标包括：

— 通过修复漏洞和通知用户来降低风险；

— 将披露所造成的损害和成本降至最低；

— 为用户提供足够的信息以评估因漏洞导致的风险；

— 设定预期以促进各利益相关方之间的合作互动与协调。

本文件中所述流程旨在将风险、成本以及对所有利益相关方造成的损害降至最低。由于报告的漏洞数量众多、缺乏准确和完整的信息以及其他相关因素，无法制定出适用于每一次披露事件的单一固定流程。

本文件中的规范性要素提供了创建功能性漏洞披露能力的最低要求。供应商应根据自身特定需求以及用户和其他利益相关方的需求，对本文件中的附加信息性指南进行调整。

信息技术 - 安全技术 - 漏洞披露

1 范围

本文件为供应商在产品和服务漏洞披露方面提供了要求和建议。漏洞披露使用户能够按照 ISO/IEC 27002:2013 中 12.6.113 节的规定执行技术漏洞管理。漏洞披露有助于用户保护其系统和数据，优先安排防御性投资，并更好地评估风险。漏洞披露的目标是降低利用漏洞所带来的风险。当多个供应商受到影响时，协调漏洞披露尤为重要。本文件提供了：

— 关于接收潜在漏洞报告的指南；

— 关于披露漏洞修复信息的指南；

— 与漏洞披露相关的术语和定义；

— 漏洞披露概念概述；

— 漏洞披露的技术和政策考量；

-- 技术、政策（附录 A）和沟通示例（附录 B）。

在接收漏洞报告和披露漏洞报告之间进行的其他相关活动在 ISO/IEC 30111 中有描述。

本文件适用于选择实施漏洞披露以降低其产品和服务用户风险的供应商。

2 规范性引用文件

文中提及的下列文件，其部分或全部内容构成本文件的要求。对于有日期的引用文件，仅适用所引用的版本。对于无日期的引用文件，适用所引用文件的最新版本（包括任何修订）。

ISO/IEC 27000 信息技术 - 安全技术 - 信息安全管理体系 - 概述和词汇表

ISO/IEC 30111 信息技术 - 安全技术 - 漏洞处理流程

3 术语和定义

就本文件而言，适用 ISO/IEC 27000 中给出的术语和定义以及以下术语和定义。

国际标准化组织（ISO）和国际电工委员会（IEC）在以下网址维护用于标准化工作的术语

— 数据库：ISO 在线浏览平台：https://www.iso.org/obp

— IEC 电气术语在线词典：网址为 http://www.electropedia.org/

如需获取全文，请联系奥邦检验认证集团客户服务部门：

1）通过邮件提出申请。请发送到邮箱：17312273399@163.com

2）也可通过客服电话咨询 025-85307007。