INTERNATIONAL STANDARD

ISO/IEC 30111

Second edition
2019-10

Information technology — Security techniques — Vulnerability handling processes

Technologies de l'information — Techniques de sécurité — Processus de traitement de la vulnérabilité

Reference number
ISO/IEC 30111:2019(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, *Information security, cybersecurity and privacy protection*.

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 second edition cancels and replaces the first edition (ISO/IEC 30111:2013), which has been technically revised. The main changes compared to the previous edition are as follows:

— a number of normative provisions have been revised or added (summarized in Annex A);

— organizational and editorial changes have been made for clarity and harmonization with ISO/IEC 29147:2018.

This document is intended to be used with ISO/IEC 29147.

Introduction

This document describes processes for vendors to handle reports of potential vulnerabilities in products and services.

The audience for this document includes developers, vendors, evaluators, and users of information technology products and services. The following audiences can use this document:

— developers and vendors, when responding to actual or potential vulnerability reports;

— evaluators, when assessing the security assurance afforded by vendors' and developers' vulnerability handling processes; and

— users, to express procurement requirements to developers, vendors and integrators.

This document is integrated with ISO/IEC 29147 at the point of receiving potential vulnerability reports and at the point of distributing vulnerability remediation information (see 5.1).

Relationships to other standards are noted in Clause 5.

Information technology — Security techniques — Vulnerability handling processes

1 Scope

This document provides requirements and recommendations for how to process and remediate reported potential vulnerabilities in a product or service.

This document is applicable to vendors involved in handling vulnerabilities.

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 29147:2018, *Information technology — Security techniques — Vulnerability disclosure*

3 Terms and definitions

For the purposes of this document, terms and definitions given in ISO/IEC 27000 and ISO/IEC 29147 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/

4 Abbreviated terms

The following abbreviated terms are used in this document.

CSIRT Computer Security Incident Response Team

PSIRT Product Security Incident Response Team

5 Relationships to other International Standards

5.1 ISO/IEC 29147

ISO/IEC 29147 shall be used in conjunction with this document. The relationship between the two is illustrated in Figure 1.

This document provides guidelines for vendors on how to process and remediate potential vulnerability information reported by internal or external individuals or organizations.

ISO/IEC 29147 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.

国际标准

ISO/IEC 30111

2019 年 10 月 第二版

信息技术 - 安全技术 - 漏洞处理流程

信息技术 - 安全技术 - 漏洞处理流程

Reference number ISO/IEC 30111:2019(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工作。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）不对识别任何此类专利权负责。在文件编制过程中所识别出的任何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，不构成任何推荐。

有关标准自愿性的说明、与合格评定相关的 ISO 特定术语和表达的含义，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（信息安全、网络安全和个人隐私保护）编制。

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。

本第二版废止并取代了第一版（ISO/IEC 30111:2013），并对其进行了技术修订。与前一版相比，主要变化如下:

— 已对若干规范性条款进行了修订或补充（详见附件 A）。

— 为了清晰明了并使内容与 ISO/IEC 29147:2018 保持一致，对组织结构和编辑内容进行了修改。

— 本文件旨在与 ISO/IEC 29147 一起使用。

引言

本文件描述了供应商处理有关产品和服务中潜在漏洞报告的流程。

本文件的受众包括信息技术产品和服务的开发人员、供应商、评估人员和用户。以下人员可以使用本文件:

— 开发人员和供应商在回应实际或潜在的安全漏洞报告时;

— 评估人员在评估供应商和开发者的漏洞处理流程所提供的安全保障时;和

— 用户可以向开发人员、供应商和集成商表达采购需求。

本文件在接收潜在漏洞报告以及分发漏洞修复信息时与 ISO/IEC 29147 相结合（见 5.1）。

与其他标准的关系在第 5 条中予以说明。

信息技术 - 安全技术 - 漏洞处理流程

1 范围

本文件提供了有关如何处理和修复产品或服务中所报告的潜在漏洞的要求和建议。

本文件适用于参与漏洞处理的供应商。

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，仅所引用的版本适用。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 概述和术语》

ISO/IEC 29147:2018《信息技术 - 安全技术 - 漏洞披露》

3 术语和定义

就本文件而言，ISO/IEC 27000 和 ISO/IEC 29147 中给出的术语和定义适用。

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：

— 国际标准化组织在线浏览平台：访问网址为 https://www.iso.org/obp

— 国际电工委员会电工术语在线词典：网址为 http://www.electropedia.org/

4 缩略语

本文件使用了以下缩略语。

计算机安全事件响应小组（CSIRT）

产品安全事件响应团队（PSIRT）

5 与其他国际标准的关系

5.1 ISO/IEC 29147

应将 ISO/IEC 29147 与本文件结合使用。两者之间的关系如图 1 所示。

本文件为供应商提供了关于如何处理和修复由内部或外部个人或组织报告的潜在漏洞信息的指导方针。

ISO/IEC 29147 为供应商提供了指南，用于在接收来自外部个人或组织的有关潜在漏洞的报告以及向受影响用户分发漏洞修复信息时纳入其常规业务流程。

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。