NORME INTERNATIONALE

ISO/IEC 30111

Deuxième édition
2019-10

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

Information technology — Security techniques — Vulnerability handling processes

Numéro de référence
ISO/IEC 30111:2019(F)

© ISO/IEC 2019



DOCUMENT PROTÉGÉ PAR COPYRIGHT

© ISO/IEC 2019

Tous droits réservés. Sauf prescription différente ou nécessité dans le contexte de sa mise en œuvre, aucune partie de cette publication ne peut être reproduite ni utilisée sous quelque forme que ce soit et par aucun procédé, électronique ou mécanique, y compris la photocopie, ou la diffusion sur l'internet ou sur un intranet, sans autorisation écrite préalable. Une autorisation peut être demandée à l'ISO à l'adresse ci-après ou au comité membre de l'ISO dans le pays du demandeur.

ISO copyright office
Case postale 401 • Ch. de Blandonnet 8
CH-1214 Vernier, Genève
Tél.: +41 22 749 01 11
Fax: +41 22 749 09 47
E-mail: copyright@iso.org
Web: www.iso.org

Publié en Suisse

Sommaire

Page

Avant-propos ..... **iv**
Introduction ..... **v**
1 Domaine d'application **1**
2 Références normatives **1**
3 Termes et définitions **1**
4 Abréviations **1**
5 Relations aux autres Normes internationales **1**
5.1 ISO/IEC 29147 1
5.2 ISO/IEC 27034 (toutes les parties) 3
5.3 ISO/IEC 27036-3 4
5.4 ISO/IEC 15408-3 4
6 Politique et cadre organisationnel **4**
6.1 Généralités 4
6.2 Leadership 4
6.2.1 Leadership et engagement 4
6.2.2 Politique 5
6.2.3 Rôles, responsabilités et autorités au sein de l'organisme 5
6.3 Élaboration de la politique de traitement des vulnérabilités 5
6.4 Développement du cadre organisationnel 5
6.5 CSIRT ou PSIRT du fournisseur 6
6.5.1 Généralités 6
6.5.2 Mission d'une PSIRT 6
6.5.3 Responsabilités d'une PSIRT 6
6.5.4 Capacités du personnel 8
6.6 Responsabilités de la division d'activités produit 8
6.7 Responsabilités du support client et des relations publiques 8
6.8 Consultation juridique 9
7 Processus de traitement des vulnérabilités **9**
7.1 Phases de traitement des vulnérabilités 9
7.1.1 Généralités 9
7.1.2 Préparation 10
7.1.3 Réception 10
7.1.4 Vérification 10
7.1.5 Développement d'une remédiation 11
7.1.6 Publication 12
7.1.7 Post-publication 12
7.2 Surveillance du processus 12
7.3 Confidentialité des informations de vulnérabilité 13
8 Considérations relatives à la chaîne d'approvisionnement **13**
Bibliographie **15**

© ISO/IEC 2019 – Tous droits réservés

Avant-propos

L'ISO (Organisation internationale de normalisation) et l'IEC (Commission électrotechnique internationale) forment le système spécialisé de la normalisation mondiale. Les organismes nationaux membres de l'ISO ou de l'IEC participent au développement de Normes internationales par l'intermédiaire des comités techniques créés par l'organisation concernée afin de s'occuper des domaines particuliers de l'activité technique. Les comités techniques de l'ISO et de l'IEC collaborent dans des domaines d'intérêt commun. D'autres organismes internationaux, gouvernementaux et non gouvernementaux, en liaison avec l'ISO et l'IEC participent également aux travaux.

Les procédures utilisées pour élaborer le présent document et celles destinées à sa mise à jour sont décrites dans les Directives ISO/IEC, Partie 1. Il convient, en particulier de prendre note des différents critères d'approbation requis pour les différents types de document. Le présent document a été rédigé conformément aux règles de rédaction données dans les Directives ISO/IEC, Partie 2 (voir www.iso.org/directives).

L'attention est attirée sur le fait que certains des éléments du présent document peuvent faire l'objet de droits de propriété intellectuelle ou de droits analogues. L'ISO et l'IEC ne sauraient être tenues pour responsables de ne pas avoir identifié de tels droits de propriété et averti de leur existence. Les détails concernant les références aux droits de propriété intellectuelle ou autres droits analogues identifiés lors de l'élaboration du document sont indiqués dans l'Introduction et/ou dans la liste des déclarations de brevets reçues par l'ISO (voir www.iso.org/brevets) ou dans la liste des déclarations de brevets reçues par l'IEC (voir https://patents.iec.c).

Les appellations commerciales éventuellement mentionnées dans le présent document sont données pour information, par souci de commodité, à l'intention des utilisateurs et ne sauraient constituer un engagement.

Pour une explication de la nature volontaire des normes, la signification des termes et expressions spécifiques de l'ISO liés à l'évaluation de la conformité, ou pour toute information au sujet de l'adhésion de l'ISO aux principes de l'Organisation mondiale du commerce (OMC) concernant les obstacles techniques au commerce (OTC), voir le lien suivant: www.iso.org/iso/fr/avant-propos.

Le présent document a été élaboré par le comité technique mixte ISO/IEC JTC 1, *Technologies de l'information*, sous-comité SC 27, *Sécurité de l'information, cybersécurité et protection de la vie privée*.

Il convient que l'utilisateur adresse tout retour d'information ou toute question concernant le présent document à l'organisme national de normalisation de son pays. Une liste exhaustive desdits organismes se trouve à l'adresse www.iso.org/fr/members.html.

Cette deuxième édition annule et remplace la première édition (ISO/IEC 30111:2013), qui a fait l'objet d'une révision technique. Les principales modifications par rapport à l'édition précédente sont les suivantes:

— certaines dispositions normatives ont été révisées ou ajoutées (synthétisées à l'Annexe A);

— des modifications organisationnelles et rédactionnelles ont été apportées à des fins de clarté et d'harmonisation avec l'ISO/IEC 29147:2018.

Le présent document est destiné à être utilisé avec l'ISO/IEC 29147.

 © ISO/IEC 2019 – Tous droits réservés

Introduction

Le présent document décrit des processus à l'attention des fournisseurs pour traiter les signalements de vulnérabilités potentielles dans leurs produits et services.

Le présent document s'adresse aux développeurs, fournisseurs, évaluateurs et utilisateurs de produits et services de technologies de l'information. Il peut être utilisé par:

— les développeurs et les fournisseurs, lorsqu'ils répondent à des signalements de vulnérabilités réelles ou potentielles;

— les évaluateurs, lorsqu'ils évaluent l'assurance de sécurité permise par les processus de traitement de vulnérabilités de fournisseurs et de développeurs;

— les utilisateurs, pour exprimer des besoins d'achat à des développeurs, des fournisseurs et des intégrateurs.

Le présent document est intégré à l'ISO/IEC 29147 au point de réception de signalements de vulnérabilités potentielles et au point de diffusion d'informations sur la remédiation de vulnérabilités (voir 5.1).

Les relations avec d'autres normes sont précisées dans l'Article 5.

© ISO/IEC 2019 – Tous droits réservés

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

1 Domaine d'application

Le présent document fournit des exigences et des recommandations sur la manière de traiter et résoudre les vulnérabilités potentielles signalées dans un produit ou un service.

Le présent document s'applique aux fournisseurs impliqués dans le traitement des vulnérabilités.

2 Références normatives

Les documents suivants cités dans le texte constituent, pour tout ou partie de leur contenu, des exigences du présent document. Pour les références datées, seule l'édition citée s'applique. Pour les références non datées, la dernière édition du document de référence s'applique (y compris les éventuels amendements).

ISO/IEC 27000, *Technologies de l'information — Techniques de sécurité — Systèmes de management de la sécurité de l'information — Vue d'ensemble et vocabulaire*

ISO/IEC 29147:2018, *Technologies de l'information — Techniques de sécurité — Divulgation de vulnérabilité*

3 Termes et définitions

Pour les besoins du présent document, les termes et définitions donnés dans l'ISO/IEC 27000 et l'ISO/IEC 29147 s'appliquent.

L'ISO et l'IEC tiennent à jour des bases de données terminologiques destinées à être utilisées en normalisation, consultables aux adresses suivantes:

— ISO Online browsing platform: disponible à l'adresse https://www.iso.org/obp

— IEC Electropedia: disponible à l'adresse http://www.electropedia.org/

4 Abréviations

Les abréviations suivantes sont utilisées dans le présent document:

CSIRT Équipe d'intervention en cas d'incidents de sécurité informatique (Computer Security Incident Response Team)

PSIRT Équipe d'intervention en cas d'incidents de sécurité produit (Product Security Incident Response Team)

5 Relations aux autres Normes internationales

5.1 ISO/IEC 29147

L'ISO/IEC 29147 doit être utilisée conjointement avec le présent document. La Figure 1 présente la relation entre les deux normes.

© ISO/IEC 2019 – Tous droits réservés