NORME INTERNATIONALE

ISO/IEC 29147

Deuxième édition
2018-10

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

Information technology — Security techniques — Vulnerability disclosure

Numéro de référence
ISO/IEC 29147:2018(F)

© ISO/IEC 2018



DOCUMENT PROTÉGÉ PAR COPYRIGHT

© ISO/IEC 2018

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 ..... **vi**
Introduction ..... **vii**
1 Domaine d'application **1**
2 Références normatives **1**
3 Termes et définitions **1**
4 Abréviations **3**
5 Concepts **3**
5.1 Généralités 3
5.2 Structure du présent document 4
5.3 Relations aux autres Normes internationales 4
5.3.1 ISO/IEC 30111 4
5.3.2 ISO/IEC 27002 5
5.3.3 Série ISO/IEC 27034 6
5.3.4 ISO/IEC 27036-3 6
5.3.5 ISO/IEC 27017 6
5.3.6 Série ISO/IEC 27035 6
5.3.7 Évaluation, test et spécification de sécurité 6
5.4 Systèmes, composants et services 6
5.4.1 Systèmes 6
5.4.2 Composants 6
5.4.3 Produits 7
5.4.4 Services 7
5.4.5 Vulnérabilité 7
5.4.6 Interdépendance des produits 8
5.5 Rôles des parties prenantes 8
5.5.1 Généralités 8
5.5.2 Utilisateur 8
5.5.3 Fournisseur 8
5.5.4 Déclarant 9
5.5.5 Coordinateur 9
5.6 Résumé du processus de traitement des vulnérabilités 10
5.6.1 Généralités 10
5.6.2 Préparation 11
5.6.3 Réception 11
5.6.4 Vérification 11
5.6.5 Développement d'une remédiation 11
5.6.6 Publication 11
5.6.7 Post-publication 12
5.6.8 Période d'embargo 12
5.7 Échange d'informations au cours de la divulgation d'une vulnérabilité 12
5.8 Confidentialité des informations échangées 13
5.8.1 Généralités 13
5.8.2 Communications sécurisées 13
5.9 Bulletins de sécurité sur des vulnérabilités 14
5.10 Exploitation de vulnérabilités 14
5.11 Vulnérabilités et risque 14
6 Réception de signalements de vulnérabilités **14**
6.1 Généralités 14
6.2 Signalements de vulnérabilités 14
6.2.1 Généralités 14
6.2.2 Capacité à recevoir des signalements 15
6.2.3 Surveillance 15

© ISO/IEC 2018 – Tous droits réservés

6.2.4 Suivi des signalements 15
6.2.5 Accusé de réception d'un signalement 16
6.3 Évaluation initiale 16
6.4 Étude complémentaire 16
6.5 Communication continue 17
6.6 Implication des coordinateurs 17
6.7 Sécurité opérationnelle 17

7 Publication de bulletins de sécurité sur des vulnérabilités 18
7.1 Généralités 18
7.2 Bulletin de sécurité 18
7.3 Période de publication d'un bulletin de sécurité 18
7.4 Éléments d'un bulletin de sécurité 19
7.4.1 Généralités 19
7.4.2 Identifiants 19
7.4.3 Date et heure 19
7.4.4 Titre 19
7.4.5 Vue d'ensemble 20
7.4.6 Produits affectés 20
7.4.7 Public cible 20
7.4.8 Localisation 20
7.4.9 Description 20
7.4.10 Impact 20
7.4.11 Gravité 21
7.4.12 Remédiation 21
7.4.13 Références 21
7.4.14 Crédit 21
7.4.15 Informations de contact 21
7.4.16 Historique des révisions 21
7.4.17 Conditions d'utilisation 21
7.5 Communication du bulletin de sécurité 21
7.6 Format du bulletin de sécurité 22
7.7 Authenticité du bulletin de sécurité 22
7.8 Remédiations 22
7.8.1 Généralités 22
7.8.2 Authenticité de la remédiation 22
7.8.3 Déploiement de remédiations 22

8 Coordination 23
8.1 Généralités 23
8.2 Fournisseurs exerçant plusieurs rôles 23
8.2.1 Généralités 23
8.2.2 Signalement de vulnérabilités entre fournisseurs 23
8.2.3 Signalement d'informations de vulnérabilités auprès d'autres fournisseurs 24

9 Politique de divulgation de vulnérabilité 24
9.1 Généralités 24
9.2 Éléments obligatoires d'une politique 24
9.2.1 Généralités 24
9.2.2 Mécanisme de contact préférentiel 24
9.3 Éléments recommandés d'une politique 25
9.3.1 Généralités 25
9.3.2 Contenu d'un signalement de vulnérabilité 25
9.3.3 Options de communications sécurisées 25
9.3.4 Définition des attentes en matière de communication 25
9.3.5 Domaine d'application 26
9.3.6 Publication 26
9.3.7 Reconnaissance 26
9.4 Éléments facultatifs d'une politique 26
9.4.1 Généralités 26

 © ISO/IEC 2018 – Tous droits réservés

9.4.2 Aspects juridiques 26
9.4.3 Délai de divulgation 26
Annexe A (informative) **Exemples de politiques de divulgation de vulnérabilités** **27**
Annexe B (informative) **Informations à demander dans un signalement** **28**
Annexe C (informative) **Exemples de bulletins de sécurité** **29**
Annexe D (informative) **Résumé des éléments normatifs** **32**
Bibliographie **34**

© ISO/IEC 2018 – 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, *Techniques de sécurité*.

Cette deuxième édition annule et remplace la première édition (ISO/IEC 29147:2014), 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 ajoutées (synthétisées à l'Annexe D);

— de nombreuses modifications organisationnelles et rédactionnelles ont été apportées pour des raisons de clarté.

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.

Le présent document est destiné à être utilisé avec l'ISO/IEC 30111.

© ISO/IEC 2018 – Tous droits réservés

Introduction

Dans les contextes des technologies de l'information et de la cybersécurité, une vulnérabilité est un comportement ou un ensemble de conditions présent dans un système, un produit, un composant ou un service, qui viole une politique de sécurité implicite ou explicite. Une vulnérabilité peut être vue comme une faille ou une exposition qui crée un impact ou une conséquence pour la sécurité. Des attaquants exploitent des vulnérabilités pour compromette la confidentialité, l'intégrité, la disponibilité, le fonctionnement ou une autre propriété de sécurité.

Les vulnérabilités sont souvent le résultat de défaillances d'un programme ou d'un système à traiter de façon sécurisée une entrée non fiable ou imprévue. Les vulnérabilités ont diverses causes, notamment des erreurs de codage ou de configuration, des négligences dans les choix de conception et des spécifications de protocole et de format non sécurisées.

En dépit d'efforts significatifs pour améliorer la sécurité des logiciels, les logiciels et systèmes modernes sont si complexes qu'il est impossible de les produire sans vulnérabilités. Les facteurs de risque des vulnérabilités comprennent:

— l'exploitation et le recours à des systèmes qui présentent des vulnérabilités connues;

— le manque d'informations suffisantes concernant des vulnérabilités;

— l'ignorance de l'existence de vulnérabilités.

Le présent document décrit des techniques et des politiques de divulgation de vulnérabilité à l'attention de fournisseurs qui reçoivent des signalements de vulnérabilités et publient des informations de remédiation. Une divulgation de vulnérabilité permet à la fois la remédiation des vulnérabilités et la prise de décisions plus avisées en matière de risque. La divulgation de vulnérabilité est un élément essentiel du support, de la maintenance et de l'exploitation de tout produit ou service exposé à des menaces actives. Cela comprend pratiquement tout produit ou service qui utilise des réseaux ouverts tels qu'Internet. Une capacité de divulgation de vulnérabilité est une partie essentielle du développement, de l'acquisition, de l'exploitation et du support de tous les produits et services. L'exploitation de produits ou services exempts de capacités de divulgation de vulnérabilité expose les utilisateurs à un risque accru.

Le terme «divulgation de vulnérabilité» est utilisé pour décrire les activités globales associées à la réception de signalements de vulnérabilités et à la fourniture d'informations sur leur remédiation. Les activités supplémentaires telles que l'enquête et la priorisation des signalements, le développement, le test et le déploiement de remédiations, ainsi que l'amélioration d'un développement sécurisé, sont appelées «traitement de vulnérabilités» et sont décrites dans l'ISO/IEC 30111. Le terme «divulgation» est aussi utilisé de façon plus restrictive pour désigner l'acte d'informer pour la première fois une partie concernant une vulnérabilité (voir 3.2).

La divulgation de vulnérabilité a plusieurs objectifs majeurs:

— réduire le risque en corrigeant des vulnérabilités et en informant les utilisateurs;

— limiter autant que possible le préjudice et le coût associés à la divulgation;

— fournir aux utilisateurs des informations suffisantes pour évaluer le risque dû à des vulnérabilités;

— définir des attentes pour faciliter l'interaction et la coordination parmi les parties prenantes.

Les processus décrits dans le présent document ont pour but de réduire autant que possible le risque, le coût et le préjudice pour l'ensemble des parties prenantes. En raison du volume de vulnérabilités signalées, du manque d'informations précises et complètes et des autres facteurs impliqués, il n'est pas possible de créer un seul processus figé qui s'applique à chaque événement de divulgation.

Les éléments normatifs du présent document fournissent des exigences minimales pour créer une capacité fonctionnelle de divulgation de vulnérabilité. Il convient que les fournisseurs adaptent les recommandations informatives du présent document à leurs besoins spécifiques ainsi qu'à ceux des utilisateurs et autres parties prenantes.

© ISO/IEC 2018 – Tous droits réservés

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

1 Domaine d'application

Le présent document fournit des exigences et des recommandations à l'attention de fournisseurs concernant la divulgation de vulnérabilités dans des produits et services. La divulgation de vulnérabilité permet aux utilisateurs d'effectuer une gestion des vulnérabilités techniques telle que spécifiée dans l'ISO/IEC 27002:2013, 12.6.1[1]. La divulgation de vulnérabilité aide les utilisateurs à protéger leurs systèmes et données, à prioriser les investissements défensifs et à mieux apprécier le risque. L'objectif d'une divulgation de vulnérabilité est de réduire le risque associé à l'exploitation de vulnérabilités. Une divulgation de vulnérabilité coordonnée est particulièrement importante lorsque plusieurs fournisseurs sont affectés. Le présent document fournit:

— des lignes directrices sur la réception de signalements concernant des vulnérabilités potentielles;

— des lignes directrices sur la divulgation d'informations concernant la remédiation de vulnérabilités;

— des termes et définitions spécifiques à la divulgation de vulnérabilités;

— une vue d'ensemble des concepts associés à la divulgation de vulnérabilité;

— des considérations relatives aux techniques et politiques de divulgation de vulnérabilité;

— des exemples de techniques, de politiques (Annexe A) et de communications (Annexe B).

D'autres activités associées intervenant entre la réception et la divulgation de signalements de vulnérabilités sont décrites dans l'ISO/IEC 30111.

Le présent document s'applique aux fournisseurs qui choisissent de pratiquer la divulgation de vulnérabilité pour réduire le risque pour les utilisateurs de produits et services de fournisseurs.

2 Références normatives

Les documents suivants sont cités dans le texte de sorte qu'ils 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 30111, *Technologies de l'information — Techniques de sécurité — Processus de traitement de la vulnérabilité*

3 Termes et définitions

Pour les besoins du présent document, les termes et définitions de l'ISO/IEC 27000 ainsi que les suivants 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

© ISO/IEC 2018 – Tous droits réservés

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

3.1
vulnérabilité
comportement fonctionnel d'un produit ou service qui viole une politique de sécurité implicite ou explicite

Note 1 à l'article: L'ISO/IEC 27002:2013, 12.6.1[1] utilise le terme «vulnérabilité technique» pour établir une distinction entre le concept plus général de vulnérabilité basée sur le risque et le terme utilisé dans le présent document.

3.2
communication
acte consistant à fournir initialement des informations relatives à une *vulnérabilité* (3.1) à une partie qui n'en avait vraisemblablement pas connaissance auparavant

3.3
coordination
ensemble d'activités comprenant l'identification et l'engagement des parties prenantes, la médiation, la communication et les autres formes de planification à l'appui d'une *divulgation* (3.2) de *vulnérabilité* (3.1)

Note 1 à l'article: Le terme «divulgation de vulnérabilité coordonnée» est utilisé pour indiquer un processus de divulgation impliquant une coordination.

3.4
fournisseur
individu ou organisme qui a la responsabilité de résoudre des vulnérabilités

Note 1 à l'article: Un fournisseur peut être le développeur, l'agent de maintenance, le producteur, le fabricant, l'approvisionneur, l'installateur ou le fournisseur d'un produit ou service.

3.5
déclarant
individu ou organisme qui informe un *fournisseur* (3.4) ou un *coordinateur* (3.6) d'une *vulnérabilité* (3.1) potentielle

Note 1 à l'article: Aucune exigence particulière ne s'applique au fait d'agir en tant que déclarant. Les déclarants peuvent être des individus, des organismes, des amateurs ou passionnés, des professionnels, des utilisateurs finaux, des organismes de recherche en sécurité, des fournisseurs, des autorités gouvernementales ou des coordinateurs.

Note 2 à l'article: Le terme «déclarant» n'implique pas une découverte ou un signalement unique ou initial(e).

Note 3 à l'article: Les déclarants peuvent être appelés «chercheurs», qu'ils mènent explicitement ou non une recherche en sécurité ou en vulnérabilités. Historiquement, le terme «découvreur» est également utilisé pour désigner ce rôle.

3.6
coordinateur
individu or organisme qui effectue une *coordination* (3.3)

3.7
remédiation
modification apportée à un produit ou service pour supprimer ou atténuer une *vulnérabilité* (3.1)

Note 1 à l'article: Une remédiation prend habituellement la forme d'un remplacement de fichier binaire, d'un changement de configuration ou d'une correction et d'une recompilation du code source. Différents termes sont utilisés pour désigner une «remédiation», par exemple patch, correctif, mise à jour, correctif d'urgence et mise à niveau. Les mesures d'atténuation sont également appelées solutions de contournement ou contremesures.

© ISO/IEC 2018 – Tous droits réservés

3.8
bulletin de sécurité
document ou message qui fournit des informations relatives à une *vulnérabilité* (3.1) destinées à en réduire le risque

Note 1 à l'article: Un bulletin de sécurité a pour but d'informer les utilisateurs ou autres parties prenantes concernant une vulnérabilité, y compris, si possible, la manière d'identifier des systèmes vulnérables et d'y remédier.

4 Abréviations

COTS	Équipement sur étagère (Common Off-The-Shelf)
CRM	Gestion de la relation client (Customer Relationship Management)
CSIRT	Équipe d'intervention en cas d'incidents de sécurité informatique (Computer Security Incident Response Team)
CVE	Vulnérabilités et expositions courantes (Common Vulnerabilities et Exposures)[9]
CVRF	Format commun de signalement de vulnérabilités (Common Vulnerability Reporting Format)[12][13]
CVSS	Système commun de classement des vulnérabilités (Common Vulnerability Scoring System)[10]
CWE	Liste des failles courantes (Common Weakness Enumeration)[11]
HTTP(S)	Protocole de transfert hypertexte (sécurisé) (Hypertext Transfer Protocol (Secure))
OpenPGP	Protocole ouvert de confidentialité PGP (Open Pretty Good Privacy)
OWASP	Projet ouvert de sécurité des applications Web (Open Web Application Security Project)
PoC	Preuve de concept (Proof of Concept)
PSIRT	Équipe d'intervention en cas d'incidents de sécurité produit (Product Security Incident Response Team)
S/MIME	Extensions de courrier électronique à multiples fins sécurisées (Secure Multipurpose Internet Mail Extensions)
SQL	Langage de requêtes structuré (Structured Query Language)
TIC	Technologies de l'Information et de la Communication
TLS	Sécurité de couche de transport (Transport Layer Security)

5 Concepts

5.1 Généralités

Le présent article a pour but de fournir des informations générales et un contexte afin de mieux comprendre le concept de divulgation de vulnérabilité.

La divulgation de vulnérabilité implique différentes parties prenantes avec des perspectives, des incitations, des capacités et des informations disponibles différentes. De plus, la communication et la synchronisation des processus parmi plusieurs parties prenantes peuvent devenir rapidement

© ISO/IEC 2018 – Tous droits réservés