



Institut luxembourgeois de la normalisation
de l'accréditation, de la sécurité et qualité
des produits et services

ILNAS-EN ISO/IEC 29147:2020

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

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

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

05/2020



Avant-propos national

Cette Norme Européenne EN ISO/IEC 29147:2020 a été adoptée comme Norme Luxembourgeoise ILNAS-EN ISO/IEC 29147:2020.

Toute personne intéressée, membre d'une organisation basée au Luxembourg, peut participer gratuitement à l'élaboration de normes luxembourgeoises (ILNAS), européennes (CEN, CENELEC) et internationales (ISO, IEC) :

- Influencer et participer à la conception de normes
- Anticiper les développements futurs
- Participer aux réunions des comités techniques

<https://portail-qualite.public.lu/fr/normes-normalisation/participer-normalisation.html>

CETTE PUBLICATION EST PROTÉGÉE PAR LE DROIT D'AUTEUR

Aucun contenu de la présente publication ne peut être reproduit ou utilisé sous quelque forme ou par quelque procédé que ce soit - électronique, mécanique, photocopie ou par d'autres moyens sans autorisation préalable !

ILNAS-EN ISO/IEC 29147:2020
NORME EUROPÉENNE **EN ISO/IEC 29147**
EUROPÄISCHE NORM
EUROPEAN STANDARD
Mai 2020

ICS 35.030

Version Française

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

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

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

La présente Norme européenne a été adoptée par le CEN le 3 mai 2020.

Les membres du CEN et CENELEC sont tenus de se soumettre au Règlement Intérieur du CEN/CENELEC, qui définit les conditions dans lesquelles doit être attribué, sans modification, le statut de norme nationale à la Norme européenne. Les listes mises à jour et les références bibliographiques relatives à ces normes nationales peuvent être obtenues auprès du Centre de Gestion du CEN-CENELEC ou auprès des membres du CEN et CENELEC.

La présente Norme européenne existe en trois versions officielles (allemand, anglais, français). Une version dans une autre langue faite par traduction sous la responsabilité d'un membre du CEN et CENELEC dans sa langue nationale et notifiée au Centre de Gestion du CEN-CENELEC, a le même statut que les versions officielles.

Les membres du CEN et du CENELEC sont les organismes nationaux de normalisation et les comités électrotechniques nationaux des pays suivants: Allemagne, Autriche, Belgique, Bulgarie, Chypre, Croatie, Danemark, Espagne, Estonie, Finlande, France, Grèce, Hongrie, Irlande, Islande, Italie, Lettonie, Lituanie, Luxembourg, Malte, Norvège, Pays-Bas, Pologne, Portugal, République de Macédoine du Nord, République de Serbie, République Tchèque, Roumanie, Royaume-Uni, Slovaquie, Slovénie, Suède, Suisse et Turquie.



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

Sommaire	Page
Avant-propos européen	3

ILNAS-EN ISO/IEC 29147:2020 - Preview only Copy via ILNAS e-Shop

Avant-propos européen

Le texte de l'ISO/IEC 29147:2018 a été élaboré par le Comité technique ISO/IEC JTC 1 « Technologies de l'information » de l'Organisation internationale de normalisation (ISO) et a été repris comme EN ISO/IEC 29147:2020 par le Comité technique CEN/CLC/JTC 13 « Cybersécurité et protection des données » dont le secrétariat est tenu par DIN.

La présente Norme européenne devra recevoir le statut de norme nationale, soit par publication d'un texte identique, soit par entérinement, au plus tard en novembre 2020 et les normes nationales en contradiction devront être retirées au plus tard en novembre 2020.

L'attention est appelée sur le fait que certains des éléments du présent document peuvent faire l'objet de droits de propriété intellectuelle ou de droits analogues. Le CEN ne saurait être tenu responsable de l'identification de tels ou tels brevets.

Selon le règlement intérieur du CEN/CENELEC, les instituts de normalisation nationaux des pays suivants sont tenus de mettre cette Norme européenne en application : Allemagne, Autriche, Belgique, Bulgarie, Chypre, Croatie, Danemark, Espagne, Estonie, Finlande, France, Grèce, Hongrie, Irlande, Islande, Italie, Lettonie, Lituanie, Luxembourg, Malte, Norvège, Pays-Bas, Pologne, Portugal, République de Macédoine du Nord, République tchèque, Roumanie, Royaume-Uni, Serbie, Slovaquie, Slovénie, Suède, Suisse et Turquie.

Notice d'entérinement

Le texte de l'ISO/IEC 29147:2018 a été approuvé par le CEN comme EN ISO/IEC 29147:2020 sans aucune modification.

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

*Information technology — Security techniques — Vulnerability
disclosure*



**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