



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

## ILNAS-EN ISO/IEC 29147:2020

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

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

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

05/2020



## National Foreword

This European Standard EN ISO/IEC 29147:2020 was adopted as Luxembourgish Standard ILNAS-EN ISO/IEC 29147:2020.

Every interested party, which is member of an organization based in Luxembourg, can participate for FREE in the development of Luxembourgish (ILNAS), European (CEN, CENELEC) and International (ISO, IEC) standards:

- Participate in the design of standards
- Foresee future developments
- Participate in technical committee meetings

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

### **THIS PUBLICATION IS COPYRIGHT PROTECTED**

Nothing from this publication may be reproduced or utilized in any form or by any mean - electronic, mechanical, photocopying or any other data carries without prior permission!

English version

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

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

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

This European Standard was approved by CEN on 3 May 2020.

CEN and CENELEC members are bound to comply with the CEN/CENELEC Internal Regulations which stipulate the conditions for giving this European Standard the status of a national standard without any alteration. Up-to-date lists and bibliographical references concerning such national standards may be obtained on application to the CEN-CENELEC Management Centre or to any CEN and CENELEC member.

This European Standard exists in three official versions (English, French, German). A version in any other language made by translation under the responsibility of a CEN and CENELEC member into its own language and notified to the CEN-CENELEC Management Centre has the same status as the official versions.

CEN and CENELEC members are the national standards bodies and national electrotechnical committees of Austria, Belgium, Bulgaria, Croatia, Cyprus, Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Iceland, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, Netherlands, Norway, Poland, Portugal, Republic of North Macedonia, Romania, Serbia, Slovakia, Slovenia, Spain, Sweden, Switzerland, Turkey and United Kingdom.



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

Contents	Page
European foreword.....	3

## European foreword

The text of ISO/IEC 29147:2018 has been prepared by Technical Committee ISO/IEC JTC 1 "Information technology" of the International Organization for Standardization (ISO) and has been taken over as EN ISO/IEC 29147:2020 by Technical Committee CEN/CLC/JTC 13 "Cybersecurity and Data Protection" the secretariat of which is held by DIN.

This European Standard shall be given the status of a national standard, either by publication of an identical text or by endorsement, at the latest by November 2020, and conflicting national standards shall be withdrawn at the latest by November 2020.

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights. CEN shall not be held responsible for identifying any or all such patent rights.

According to the CEN-CENELEC Internal Regulations, the national standards organizations of the following countries are bound to implement this European Standard: Austria, Belgium, Bulgaria, Croatia, Cyprus, Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Iceland, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, Netherlands, Norway, Poland, Portugal, Republic of North Macedonia, Romania, Serbia, Slovakia, Slovenia, Spain, Sweden, Switzerland, Turkey and the United Kingdom.

## Endorsement notice

The text of ISO/IEC 29147:2018 has been approved by CEN as EN ISO/IEC 29147:2020 without any modification.

---

---

## **Information technology — Security techniques — Vulnerability disclosure**

*Technologies de l'information — Techniques de sécurité —  
Divulgateion de vulnérabilité*



**COPYRIGHT PROTECTED DOCUMENT**

© ISO/IEC 2018

All rights reserved. Unless otherwise specified, or required in the context of its implementation, no part of this publication may be reproduced or utilized otherwise in any form or by any means, electronic or mechanical, including photocopying, or posting on the internet or an intranet, without prior written permission. Permission can be requested from either ISO at the address below or ISO's member body in the country of the requester.

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](mailto:copyright@iso.org)  
Website: [www.iso.org](http://www.iso.org)

Published in Switzerland

# Contents

Page

<b>Foreword</b>	<b>vi</b>
<b>Introduction</b>	<b>vii</b>
<b>1 Scope</b>	<b>1</b>
<b>2 Normative references</b>	<b>1</b>
<b>3 Terms and definitions</b>	<b>1</b>
<b>4 Abbreviated terms</b>	<b>3</b>
<b>5 Concepts</b>	<b>3</b>
5.1 General	3
5.2 Structure of this document	3
5.3 Relationships to other International Standards	4
5.3.1 ISO/IEC 30111	4
5.3.2 ISO/IEC 27002	5
5.3.3 ISO/IEC 27034 series	6
5.3.4 ISO/IEC 27036-3	6
5.3.5 ISO/IEC 27017	6
5.3.6 ISO/IEC 27035 series	6
5.3.7 Security evaluation, testing and specification	6
5.4 Systems, components, and services	6
5.4.1 Systems	6
5.4.2 Components	6
5.4.3 Products	6
5.4.4 Services	7
5.4.5 Vulnerability	7
5.4.6 Product interdependency	7
5.5 Stakeholder roles	8
5.5.1 General	8
5.5.2 User	8
5.5.3 Vendor	8
5.5.4 Reporter	8
5.5.5 Coordinator	9
5.6 Vulnerability handling process summary	9
5.6.1 General	9
5.6.2 Preparation	10
5.6.3 Receipt	10
5.6.4 Verification	11
5.6.5 Remediation development	11
5.6.6 Release	11
5.6.7 Post-release	12
5.6.8 Embargo period	12
5.7 Information exchange during vulnerability disclosure	12
5.8 Confidentiality of exchanged information	13
5.8.1 General	13
5.8.2 Secure communications	13
5.9 Vulnerability advisories	13
5.10 Vulnerability exploitation	14
5.11 Vulnerabilities and risk	14
<b>6 Receiving vulnerability reports</b>	<b>14</b>
6.1 General	14
6.2 Vulnerability reports	14
6.2.1 General	14
6.2.2 Capability to receive reports	14
6.2.3 Monitoring	15