

ILNAS

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

ILNAS-EN ISO/IEC 29147:2020

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

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

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

05/2020

A decorative graphic in the bottom right corner featuring several interlocking gears in shades of blue and yellow. Overlaid on the gears are binary code strings (0s and 1s) and mathematical symbols like plus and minus signs, suggesting a technical or digital theme.

Nationales Vorwort

Diese Europäische Norm EN ISO/IEC 29147:2020 wurde als luxemburgische Norm ILNAS-EN ISO/IEC 29147:2020 übernommen.

Alle interessierten Personen, welche Mitglied einer luxemburgischen Organisation sind, können sich kostenlos an der Entwicklung von luxemburgischen (ILNAS), europäischen (CEN, CENELEC) und internationalen (ISO, IEC) Normen beteiligen:

- Inhalt der Normen beeinflussen und mitgestalten
- Künftige Entwicklungen vorhersehen
- An Sitzungen der technischen Komitees teilnehmen

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

DIESES WERK IST URHEBERRECHTLICH GESCHÜTZT

Kein Teil dieser Veröffentlichung darf ohne schriftliche Einwilligung weder vervielfältigt noch in sonstiger Weise genutzt werden - sei es elektronisch, mechanisch, durch Fotokopien oder auf andere Art!

ICS 35.030

Deutsche Fassung

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

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

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

Diese Europäische Norm wurde vom CEN am 3. Mai 2020 angenommen.

Die CEN und CENELEC-Mitglieder sind gehalten, die CEN/CENELEC-Geschäftsordnung zu erfüllen, in der die Bedingungen festgelegt sind, unter denen dieser Europäischen Norm ohne jede Änderung der Status einer nationalen Norm zu geben ist. Auf dem letzten Stand befindliche Listen dieser nationalen Normen mit ihren bibliographischen Angaben sind beim CEN-CENELEC-Management-Zentrum oder bei jedem CEN und CENELEC-Mitglied auf Anfrage erhältlich.

Diese Europäische Norm besteht in drei offiziellen Fassungen (Deutsch, Englisch, Französisch). Eine Fassung in einer anderen Sprache, die von einem CEN und CENELEC-Mitglied in eigener Verantwortung durch Übersetzung in seine Landessprache gemacht und dem Management-Zentrum mitgeteilt worden ist, hat den gleichen Status wie die offiziellen Fassungen.

CEN- und CENELEC-Mitglieder sind die nationalen Normungsinstitute und elektrotechnischen Komitees von Belgien, Bulgarien, Dänemark, Deutschland, Estland, Finnland, Frankreich, Griechenland, Irland, Island, Italien, Kroatien, Lettland, Litauen, Luxemburg, Malta, den Niederlanden, Norwegen, Österreich, Polen, Portugal, der Republik Nordmazedonien, Rumänien, Schweden, der Schweiz, Serbien, der Slowakei, Slowenien, Spanien, der Tschechischen Republik, der Türkei, Ungarn, dem Vereinigten Königreich und Zypern.



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

Inhalt

	Seite
Europäisches Vorwort	5
Vorwort	6
Einleitung	7
1 Anwendungsbereich	9
2 Normative Verweisungen	9
3 Begriffe	9
4 Abkürzungen	11
5 Konzepte	11
5.1 Allgemeines	11
5.2 Struktur dieses Dokuments	12
5.3 Zusammenhänge mit anderen Internationalen Normen	12
5.3.1 ISO/IEC 30111	12
5.3.2 ISO/IEC 27002	13
5.3.3 Normenreihe ISO/IEC 27034	14
5.3.4 ISO/IEC 27036-3	14
5.3.5 ISO/IEC 27017	14
5.3.6 Normenreihe ISO/IEC 27035	14
5.3.7 Sicherheitsbewertung, Prüfung und Spezifikation	14
5.4 Systeme, Komponenten und Dienstleistungen	14
5.4.1 Systeme	14
5.4.2 Komponenten	14
5.4.3 Produkte	15
5.4.4 Dienstleistungen	15
5.4.5 Schwachstelle	15
5.4.6 Wechselseitige Produktabhängigkeit	16
5.5 Rollen der Beteiligten	16
5.5.1 Allgemeines	16
5.5.2 Anwender	16
5.5.3 Anbieter	16
5.5.4 Berichtersteller	17
5.5.5 Koordinator	17
5.6 Zusammenfassung des Schwachstellenbehandlungsprozesses	18
5.6.1 Allgemeines	18
5.6.2 Vorbereitung	19
5.6.3 Empfang	19
5.6.4 Verifizierung	20
5.6.5 Entwickeln der Problembhebung	20
5.6.6 Freigabe	20
5.6.7 Nach der Freigabe	21
5.6.8 Sperrfrist	21
5.7 Informationsaustausch während der Offenlegung von Schwachstellen	21
5.8 Vertraulichkeit von ausgetauschten Informationen	22
5.8.1 Allgemeines	22
5.8.2 Sichere Kommunikationswege	22
5.9 Beratende Dokumente über Schwachstellen	23

5.10	Ausnutzung einer Schwachstelle	23
5.11	Schwachstellen und Risiko	23
6	Empfangen von Schwachstellenberichten	23
6.1	Allgemeines	23
6.2	Schwachstellenberichte	23
6.2.1	Allgemeines	23
6.2.2	Fähigkeit zum Empfangen von Berichten.....	24
6.2.3	Überwachung	24
6.2.4	Berichtsverfolgung	25
6.2.5	Bestätigung des Berichts	25
6.3	Erstbeurteilung	25
6.4	Weitere Untersuchungen.....	26
6.5	Fortlaufende Kommunikation	26
6.6	Beteiligung von Koordinatoren.....	26
6.7	Betriebssicherheit.....	27
7	Veröffentlichen von beratenden Dokumenten	27
7.1	Allgemeines	27
7.2	Beratendes Dokument.....	27
7.3	Zeitplan für die Veröffentlichung von beratenden Dokumenten	27
7.4	Elemente von beratenden Dokumenten	28
7.4.1	Allgemeines	28
7.4.2	Kennungen	29
7.4.3	Datum und Uhrzeit.....	29
7.4.4	Titel.....	29
7.4.5	Überblick	29
7.4.6	Betroffene Produkte.....	29
7.4.7	Vorgesehene Zielgruppe	30
7.4.8	Lokalisierung	30
7.4.9	Beschreibung	30
7.4.10	Auswirkung.....	30
7.4.11	Schweregrad.....	30
7.4.12	Problembhebung.....	31
7.4.13	Verweisungen	31
7.4.14	Anerkennung	31
7.4.15	Kontaktinformationen.....	31
7.4.16	Versionshistorie.....	31
7.4.17	Nutzungsbedingungen	31
7.5	Übermittlung des beratenden Dokuments	31
7.6	Format des beratenden Dokuments.....	32
7.7	Authentizität von beratenden Dokumenten	32
7.8	Problembhebungen.....	32
7.8.1	Allgemeines	32
7.8.2	Authentizität der Problembhebung	32
7.8.3	Durchführung von Problembhebungen.....	32
8	Koordination.....	33
8.1	Allgemeines	33
8.2	Anbieter mit verschiedenen Rollen	33
8.2.1	Allgemeines	33
8.2.2	Schwachstellenberichterstattung zwischen Anbietern.....	33
8.2.3	Berichten von Schwachstelleninformationen an andere Anbieter.....	34
9	Richtlinie über die Offenlegung von Schwachstellen.....	34
9.1	Allgemeines	34
9.2	Erforderliche Richtlinienelemente.....	34
9.2.1	Allgemeines	34

9.2.2 Bevorzugte Kontaktaufnahmeverfahren..... 35

9.3 Empfohlene Richtlinienelemente 35

9.3.1 Allgemeines 35

9.3.2 Inhalte des Schwachstellenberichts 35

9.3.3 Sichere Kommunikationsoptionen 35

9.3.4 Festlegen von Anforderungen an die Kommunikation..... 36

9.3.5 Anwendungsbereich..... 36

9.3.6 Veröffentlichung 36

9.3.7 Würdigung..... 36

9.4 Optionale Richtlinienelemente 36

9.4.1 Allgemeines 36

9.4.2 Rechtliche Aspekte..... 36

9.4.3 Zeitplan für die Offenlegung..... 36

Anhang A (informativ) Beispiele für Richtlinien über die Offenlegung von Schwachstellen..... 37

Anhang B (informativ) In einem Bericht erforderliche Informationen 38

Anhang C (informativ) Beispiele für beratende Dokumente..... 39

Anhang D (informativ) Zusammenfassung der normativen Elemente..... 42

Literaturhinweise..... 44

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

Europäisches Vorwort

Der Text von ISO/IEC 29147:2018 wurde vom Technischen Komitee ISO/IEC JTC 1 „Information technology“ der Internationalen Organisation für Normung (ISO) erarbeitet und als EN ISO/IEC 29147:2020 durch das Technische Komitee CEN/CLC/JTC 13 „Cybersicherheit und Datenschutz“ übernommen, dessen Sekretariat von DIN gehalten wird.

Diese Europäische Norm muss den Status einer nationalen Norm erhalten, entweder durch Veröffentlichung eines identischen Textes oder durch Anerkennung bis November 2020, und etwaige entgegenstehende nationale Normen müssen bis November 2020 zurückgezogen werden.

Es wird auf die Möglichkeit hingewiesen, dass einige Elemente dieses Dokuments Patentrechte berühren können. CEN ist nicht dafür verantwortlich, einige oder alle diesbezüglichen Patentrechte zu identifizieren.

Entsprechend der CEN-CENELEC-Geschäftsordnung sind die nationalen Normungsinstitute der folgenden Länder gehalten, diese Europäische Norm zu übernehmen: Belgien, Bulgarien, Dänemark, Deutschland, die Republik Nordmazedonien, Estland, Finnland, Frankreich, Griechenland, Irland, Island, Italien, Kroatien, Lettland, Litauen, Luxemburg, Malta, Niederlande, Norwegen, Österreich, Polen, Portugal, Rumänien, Schweden, Schweiz, Serbien, Slowakei, Slowenien, Spanien, Tschechische Republik, Türkei, Ungarn, Vereinigtes Königreich und Zypern.

Anerkennungsnotiz

Der Text von ISO/IEC 29147:2018 wurde von CEN als EN ISO/IEC 29147:2020 ohne irgendeine Abänderung genehmigt.

Vorwort

ISO (die Internationale Organisation für Normung) und IEC (die Internationale Elektrotechnische Kommission) bilden das auf die weltweite Normung spezialisierte System. Nationale Normungsorganisationen, die Mitglieder von ISO oder IEC sind, beteiligen sich an der Entwicklung von Internationalen Normen in Technischen Komitees, die von der jeweiligen Organisation eingerichtet wurden, um spezifische Gebiete technischer Aktivitäten zu behandeln. Auf Gebieten von beiderseitigem Interesse arbeiten die Technischen Komitees von ISO und IEC zusammen. Weitere internationale staatliche und nichtstaatliche Organisationen, die in engem Kontakt mit ISO und IEC stehen, nehmen ebenfalls an der Arbeit teil.

Die Verfahren, die bei der Entwicklung dieses Dokuments angewendet wurden und die für die weitere Pflege vorgesehen sind, werden in den ISO/IEC-Direktiven, Teil 1 beschrieben. Im Besonderen sollten die für die verschiedenen ISO-Dokumentenarten notwendigen Annahmekriterien beachtet werden. Dieses Dokument wurde in Übereinstimmung mit den Gestaltungsregeln der ISO/IEC-Direktiven, Teil 2 erarbeitet (siehe www.iso.org/directives).

Es wird auf die Möglichkeit hingewiesen, dass einige Elemente dieses Dokuments Patentrechte berühren können. ISO und IEC sind nicht dafür verantwortlich, einige oder alle diesbezüglichen Patentrechte zu identifizieren. Details zu allen während der Entwicklung des Dokuments identifizierten Patentrechten finden sich in der Einleitung und/oder in der ISO-Liste der erhaltenen Patenterklärungen (siehe www.iso.org/patents).

Jeder in diesem Dokument verwendete Handelsname dient nur zur Unterrichtung der Anwender und bedeutet keine Anerkennung.

Für eine Erläuterung des freiwilligen Charakters von Normen, der Bedeutung ISO-spezifischer Begriffe und Ausdrücke in Bezug auf Konformitätsbewertungen sowie Informationen darüber, wie ISO die Grundsätze der Welthandelsorganisation (WTO, en: World Trade Organization) hinsichtlich technischer Handelshemmnisse (TBT, en: Technical Barriers to Trade) berücksichtigt, siehe www.iso.org/iso/foreword.html.

Dieses Dokument wurde vom gemeinsamen Technischen Komitee ISO/IEC JTC 1, *Information technology*, Unterkomitee SC 27, *Security techniques* erarbeitet.

Diese zweite Ausgabe ersetzt die erste Ausgabe (ISO/IEC 29147:2014), die technisch überarbeitet wurde.

Die wesentlichen Änderungen im Vergleich zur Vorgängerausgabe sind folgende:

- es wurden einige normative Festlegungen hinzugefügt (zusammengefasst in Anhang D);
- zahlreiche organisatorische und redaktionelle Änderungen wurden zur Verdeutlichung vorgenommen.

Rückmeldungen oder Fragen zu diesem Dokument sollten an das jeweilige nationale Normungsinstitut des Anwenders gerichtet werden. Eine vollständige Auflistung dieser Institute ist unter www.iso.org/members.html zu finden.

Dieses Dokument soll zusammen mit ISO/IEC 30111 angewendet werden.