ILNAS

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

ILNAS-EN ISO/IEC 30111:2020

Informationstechnik - IT-Sicherheitsverfahren - Prozesse für die Behandlung von Schwachstellen (ISO/IEC 30111:2019)

Technologies de l'information - Techniques de sécurité - Processus de traitement de la vulnérabilité (ISO/IEC 30111:2019)

Information technology - Security techniques - Vulnerability handling processes (ISO/IEC 30111:2019)

05/2020

Nationales Vorwort

Diese Europäische Norm EN ISO/IEC 30111:2020 wurde als luxemburgische Norm ILNAS-EN ISO/IEC 30111:2020 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

EUROPÄISCHE NORM
EUROPEAN STANDARD
NORME EUROPÉENNE

EN ISO/IEC 30111

Mai 2020

ICS 35.030

Deutsche Fassung

Informationstechnik - IT-Sicherheitsverfahren - Prozesse für die Behandlung von Schwachstellen (ISO/IEC 30111:2019)

Information technology - Security techniques - Vulnerability handling processes (ISO/IEC 30111:2019)

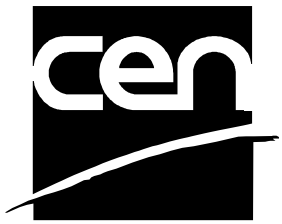
Technologies de l'information - Techniques de sécurité - Processus de traitement de la vulnérabilité (ISO/IEC 30111:2019)

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

Europäisches Vorwort

Der Text von ISO/IEC 30111:2019 wurde vom Technischen Komitee ISO/IEC JTC 1 „Information technology“ der Internationalen Organisation für Normung (ISO) erarbeitet und als EN ISO/IEC 30111:2020 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 30111:2019 wurde von CEN als EN ISO/IEC 30111:2020 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) oder in der IEC-Liste der erhaltenen Patenterklärungen (siehe http://patents.iec.ch).

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 Technischen Komitee ISO/IEC JTC 1, *Information technology,* Unterkomitee SC 27, *Information security, cybersecurity and privacy protection,* erarbeitet.

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.

Diese zweite Ausgabe ersetzt die erste Ausgabe (ISO/IEC 30111:2013), die technisch überarbeitet wurde. Die wesentlichen Änderungen im Vergleich zur Vorgängerausgabe sind folgende:

— einige der normativen Bestimmungen wurden überarbeitet oder hinzugefügt (in Anhang A zusammengefasst);

— organisatorische und redaktionelle Änderungen wurden zur besseren Verständlichkeit sowie zur Harmonisierung mit ISO/IEC 29147:2018 vorgenommen.

Dieses Dokument ist für die Verwendung im Zusammenhang mit ISO/IEC 29147 vorgesehen.

Einleitung

In diesem Dokument werden Prozesse für Anbieter für die Bearbeitung von Meldungen über potentielle Schwachstellen bei Produkten und Dienstleistungen beschrieben.

Die Zielgruppe dieses Dokuments besteht unter anderem aus Entwicklern, Lieferanten, Evaluatoren und Anwendern von Produkten und Dienstleistungen der Informationstechnologie. Die folgenden Zielgruppen können dieses Dokument verwenden:

— Entwickler und Lieferanten bei der Reaktion auf Meldungen über tatsächliche oder potentielle Schwachstellen;

— Evaluatoren bei der Bewertung der Sicherheitszusagen, die die Bearbeitungsprozesse der Lieferanten und Entwickler bei Schwachstellen bieten; und

— Anwender bei der Formulierung von Beschaffungsanforderungen an Entwickler, Lieferanten und Integratoren.

Dieses Dokument ist ein Bestandteil von ISO/IEC 29147 zum Empfangszeitpunkt von Meldungen über potentielle Schwachstellen und zum Zeitpunkt der Verteilung von Abhilfemaßnahmen für Schwachstellen (siehe 5.1).

Beziehungen zu anderen Normen sind in Abschnitt 5 aufgeführt.

1 Anwendungsbereich

In diesem Dokument werden Anforderungen und Empfehlungen für die Bearbeitung und Behebung von gemeldeten potentiellen Schwachstellen bei Produkten oder Dienstleistungen festgelegt.

Dieses Dokument gilt für Lieferanten, die an der Bearbeitung von Schwachstellen beteiligt sind.

2 Normative Verweisungen

Die folgenden Dokumente werden im Text in solcher Weise in Bezug genommen, dass einige Teile davon oder ihr gesamter Inhalt Anforderungen des vorliegenden Dokuments darstellen. Bei datierten Verweisungen gilt nur die in Bezug genommene Ausgabe. Bei undatierten Verweisungen gilt die letzte Ausgabe des in Bezug genommenen Dokuments (einschließlich aller Änderungen).

ISO/IEC 27000, *Information technology — Security techniques — Information security management systems — Overview and vocabulary*

ISO/IEC 29147:2018, *Information technology — Security techniques — Vulnerability disclosure*

3 Begriffe

Für die Anwendung dieses Dokuments gelten die Begriffe nach ISO/IEC 27000 und ISO/IEC 29147.

ISO und IEC stellen terminologische Datenbanken für die Verwendung in der Normung unter den folgenden Adressen bereit:

— ISO Online Browsing Platform: verfügbar unter https://www.iso.org/obp

— IEC Electropedia: verfügbar unter http://www.electropedia.org/

4 Abkürzungen

Die folgenden Abkürzungen werden in diesem Dokument verwendet.

CSIRT Reaktionsteam für Computersicherheitsvorfälle (en: Computer Security Incident Response Team)

PSIRT Reaktionsteam für Produktsicherheitsvorfälle (en: Product Security Incident Response Team)

5 Beziehungen zu anderen Internationalen Normen

5.1 ISO/IEC 29147

Dieses Dokument muss zusammen mit ISO/IEC 29147 verwendet werden. Die Beziehung zwischen diesen beiden Dokumenten ist in Bild 1 dargestellt.

In diesem Dokument werden Leitfäden für Lieferanten beschrieben, wie Informationen über potentielle Schwachstellen bearbeitet und beseitigt werden können, die von internen oder externen Einzelpersonen oder Organisationen gemeldet werden.

ISO/IEC 29147 enthält Leitlinien für Lieferanten, die diese in ihre üblichen Geschäftsprozesse einbinden können, wenn sie Meldungen über potentielle Schwachstellen von externen Einzelpersonen oder Organisationen erhalten, und wenn sie Informationen über die Beseitigung von Schwachstellen an betroffene Anwender verteilen.