ICS 35.030 SLOVENSKÁ TECHNICKÁ NORMA November 2024

STN	**Informačné technológie Bezpečnostné metódy Procesy riešenia zraniteľností (ISO/IEC 30111: 2019)**	**STN EN ISO/IEC 30111 97 4189**

Information technology
Security techniques
Vulnerability handling processes

Technologies de l'information
Techniques de sécurité
Processus de traitement de la vulnérabilité

Informationstechnik
IT-Sicherheitsverfahren
Prozesse für die Behandlung von Schwachstellen

Táto slovenská technická norma je slovenskou verziou európskej normy EN ISO/IEC 30111: 2020.
Preklad zabezpečil Úrad pre normalizáciu, metrológiu a skúšobníctvo Slovenskej republiky.
STN EN ISO/IEC 30111 má rovnaké postavenie, ako majú oficiálne verzie.

This standard is the Slovak version of the European Standard EN ISO/IEC 30111: 2020.
It was translated by Slovak Office of Standards, Metrology and Testing.
STN EN ISO/IEC 30111 has the same status as the official versions.

Nahradenie predchádzajúcich dokumentov

Táto slovenská technická norma nahrádza anglickú verziu STN EN ISO/IEC 30111
z novembra 2020 v celom rozsahu.

139227

Národný predhovor

Obrázky a matematické výrazy v tejto STN sú prevzaté z elektronických podkladov dodaných z ISO, © 2019 ISO, ref. č. ISO/IEC 30111: 2019 E.

Toto druhé vydanie ruší a nahrádza prvé vydanie (ISO/IEC 30111: 2013), ktoré bolo technicky revidované. Hlavné zmeny v porovnaní s predchádzajúcim vydaním sú tieto:

- bolo revidovaných alebo doplnených niekoľko normatívnych ustanovení (súhrnne v prílohe A);
- organizačné a redakčné zmeny boli vykonané z dôvodu prehľadnosti a harmonizácie s normou ISO/IEC 29147: 2018.

Tento dokument je určený na použitie s normou ISO/IEC 29147.

Normatívne referenčné dokumenty

Na nasledujúce dokumenty sa odkazuje v texte takým spôsobom, že časť ich obsahu alebo celý obsah predstavuje požiadavky tohto dokumentu. Pri datovaných odkazoch sa používa len citované vydanie. Pri nedatovaných odkazoch sa používa najnovšie vydanie citovaného dokumentu (vrátane akýchkoľvek zmien).

POZNÁMKA 1. – Ak bola medzinárodná publikácia zmenená spoločnými modifikáciami, čo je indikované označením (mod), použije sa príslušná EN/HD.

POZNÁMKA 2. – Aktuálne informácie o platných a zrušených STN a TNI možno získať na webovom sídle www.unms.sk.

ISO/IEC 27000 prijatá ako STN EN ISO/IEC 27000 Informačné technológie. Bezpečnostné metódy. Systémy riadenia informačnej bezpečnosti. Prehľad a slovník (ISO/IEC 27000: 2018) (97 4170)

ISO/IEC 29147: 2018 prijatá ako STN EN ISO/IEC 29147: 2024 Informačné technológie. Bezpečnostné metódy. Zverejňovanie zraniteľnosti (ISO/IEC 29147: 2018) (97 4192)

Vypracovanie

Spracovateľ: SynCo, s.r.o., Bratislava, Ing. Lenka Gondová

Technická komisia: TK 37 Informačné technológie

EURÓPSKA NORMA **EN ISO/IEC 30111**
EUROPEAN STANDARD
NORME EUROPÉENNE
EUROPÄISCHE NORM Máj 2020

ICS 35.030

Informačné technológie Bezpečnostné metódy Procesy riešenia zraniteľnosí (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)

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

Túto európsku normu schválil CEN 3. mája 2020.

Členovia CEN a CENELEC sú povinní plniť vnútorné predpisy CEN/CENELEC, v ktorých sú určené podmienky, za ktorých sa tejto európskej norme bez akýchkoľvek zmien priznáva postavenie národnej normy. Aktualizované zoznamy a bibliografické odkazy týkajúce sa takýchto národných noriem možno na požiadanie dostať od Riadiaceho strediska CEN-CENELEC alebo od každého člena CEN.

Táto európska norma existuje v troch oficiálnych verziách (anglickej, francúzskej, nemeckej). Verzia v akomkoľvek inom jazyku, ktorú na vlastnú zodpovednosť vydal člen CEN a CENELEC v preklade do národného jazyka a ktorá bola oznámená Riadiacemu stredisku CEN-CENELEC, má rovnaké postavenie, ako majú oficiálne verzie.

Členmi CEN a CENELEC sú národné normalizačné organizácie Belgicka, Bulharska, Cypru, Česka, Dánska, Estónska, Fínska, Francúzska, Grécka, Holandska, Chorvátska, Írska, Islandu, Litvy, Lotyšska, Luxemburska, Maďarska, Malty, Nemecka, Nórska, Poľska, Portugalska, Rakúska, Rumunska, Severného Macedónska, Slovenska, Slovinska, Spojeného kráľovstva, Srbska, Španielska, Švajčiarska, Švédska, Talianska a Turecka.

CEN

Európsky výbor pre normalizáciu
European Committee for Standardization
Comité Européen de Normalisation
Europäisches Komitee für Normung

CENELEC

Európsky výbor pre normalizáciu v elektrotechnike
European Committee for Electrotechnical Standardization
Comité Européen de Normalisation Electrotechnique
Europäisches Komitee für Elektrotechnische Normung

Riadiace stredisko CEN-CENELEC: Rue de la Science 23, B-1040 Brusel

Ref. č. EN ISO/IEC 30111: 2020 SK

Obsah

strana

Európsky predhovor

Tento dokument (ISO/IEC 30111: 2019) vypracovala technická komisia ISO/IEC JTC 1 Informačné technológie medzinárodnej organizácie pre normalizáciu (ISO) a bol prevzatý ako EN ISO/IEC 30111: 2020 technickou komisiou CEN/CLC/JTC 13 Kybernetická bezpečnosť a ochrana súkromia, ktorej sekretariát je v DIN.

Tejto európskej norme sa musí priznať postavenie národnej normy buď vydaním identického textu, alebo oznámením najneskôr do novembra 2020 a národné normy, ktoré sú s ňou v rozpore, musia sa zrušiť najneskôr do novembra 2020.

Upozorňuje sa na možnosť, že niektoré časti tohto dokumentu môžu byť predmetom patentových práv. CEN nezodpovedá za identifikáciu ktoréhokoľvek alebo všetkých takýchto patentových práv.

V súlade s vnútornými predpismi CEN-CENELEC sú túto európsku normu povinné prevziať národné normalizačné organizácie týchto krajín: Belgicka, Bulharska, Cypru, Česka, Dánska, Estónska, Fínska, Francúzska, Grécka, Holandska, Chorvátska, Írska, Islandu, Litvy, Lotyšska, Luxemburska, Maďarska, Malty, Nemecka, Nórska, Poľska, Portugalska, Rakúska, Rumunska, Severného Macedónska, Slovenska, Slovinska, Spojeného kráľovstva, Srbska, Španielska, Švajčiarska, Švédska, Talianska a Turecka.

Oznámenie o schválení

Text medzinárodnej normy ISO/IEC 30111: 2019 schválil CEN ako EN ISO/IEC 30111: 2020 bez akýchkoľvek modifikácií.

Úvod

V tomto dokumente sú opísané postupy, ktorými sa majú dodávatelia zaoberať pri nahlasovaní potenciálnych zraniteľností produktov a služieb.

Tento dokument je určený pre vývojárov, dodávateľov, hodnotiteľov a používateľov produktov a služieb informačných technológií. Tento dokument môžu používať nasledovné skupiny používateľov:

- vývojári a dodávatelia pri reakcii na skutočné alebo potenciálne hlásenia o zraniteľnostiach;
- hodnotitelia pri posudzovaní bezpečnostnej záruky, ktorú poskytujú postupy dodávateľov a vývojárov pri riešení zraniteľností; a
- používatelia, na vyjadrenie požiadavky na obstarávanie vývojárom, dodávateľom a integrátorom.

Tento dokument je integrovaný s normou ISO/IEC 29147 v bode prijímania hlásení o potenciálnych zraniteľnostiach a v bode distribúcie informácií o odstraňovaní zraniteľností (pozri 5.1).

Vzťahy k iným normám sú uvedené v kapitole 5.

1 Predmet

Tento dokument obsahuje požiadavky a odporúčania na spracovanie a nápravu nahlásených potenciálnych zraniteľností produktu alebo služby.

Tento dokument sa vzťahuje na dodávateľov, zapojených do riešenia zraniteľností.

2 Normatívne odkazy

Na nasledujúce dokumenty sa odkazuje v texte takým spôsobom, že časť ich obsahu alebo celý obsah predstavuje požiadavky tohto dokumentu. Pri datovaných odkazoch sa používa len citované vydanie. Pri nedatovaných odkazoch sa používa najnovšie vydanie citovaného dokumentu (vrátane akýchkoľvek zmien).

ISO/IEC 27000 *Information technology – Security techniques – Information security management systems – Overview and vocabulary.* [Informačné technológie. Bezpečnostné metódy. Systémy riadenia informačnej bezpečnosti. Prehľad a slovník.]

ISO/IEC 29147: 2018 *Information technology – Security techniques – Vulnerability disclosure.* [Informačné technológie. Bezpečnostné metódy. Odhaľovanie zraniteľnosti.]