ICS 35.030 SLOVENSKÁ TECHNICKÁ NORMA December 2024

STN	**Informačné technológie Bezpečnostné metódy Zverejňovanie zraniteľností (ISO/IEC 29147: 2018)**	**STN EN ISO/IEC 29147 97 4192**

Information technology
Security techniques
Vulnerability disclosure

Technologies de l'information
Techniques de sécurité
Divulgation de vulnérabilité

Informationstechnik
Sicherheitstechniken
Offenlegung von Schwachstellen

Táto slovenská technická norma je slovenskou verziou európskej normy EN ISO/IEC 29147: 2020.
Preklad zabezpečil Úrad pre normalizáciu, metrológiu a skúšobníctvo Slovenskej republiky.
STN EN ISO/IEC 29147 má rovnaké postavenie, ako majú oficiálne verzie.

This standard is the Slovak version of the European Standard EN ISO/IEC 29147: 2020.
It was translated by Slovak Office of Standards, Metrology and Testing.
STN EN ISO/IEC 29147 has the same status as the official versions.

Nahradenie predchádzajúcich dokumentov

Táto slovenská technická norma nahrádza anglickú verziu STN EN ISO/IEC 29147 z novembra 2020 v celom rozsahu.

139491

Národný predhovor

Obrázky a matematické výrazy v tejto STN sú prevzaté z elektronických podkladov dodaných z ISO/IEC, © 2018 ISO/IEC, ref. č. ISO/IEC 29147: 2018 E.

Toto druhé vydanie ruší a nahrádza prvé vydanie (ISO/IEC 29147: 2014), ktoré bolo technicky revidované.

Hlavné zmeny oproti predchádzajúcemu vydaniu sú nasledovné:

- bol pridaný rad normatívnych ustanovení (zhrnuté v prílohe D);
- bolo vykonaných mnoho organizačných a redakčných zmien s cieľom zlepšiť prehľadnosť.

Tento dokument je určený na použitie spolu s ISO/IEC 30111.

Preklad medzinárodnej normy musí získať konsolidovaný význam v obidvoch jazykoch. Nie je vždy možné a žiaduce vykonať preklad odborného kontextu doslovným prekladom, spájaním viet a gramatickými zámenami slov. Z toho dôvodu boli pri preklade tejto medzinárodnej normy použité aj lexikálno-gramatické postupy, najmä explikácia (opisný preklad), s cieľom čo najväčšieho zachovania významovej stránky obsahu za cenu zmien jeho výrazovej stránky za použitia primeraných výrazových prostriedkov.

Ak sa v časti literatúra uvádza taká norma, ktorá je už prevzatá do sústavy STN, je namiesto doslovného prekladu názvu normy použitý jej platný názov, v tvare, v akom bol schválený a publikovaný v sústave STN.

Niektoré termíny sú preložené v iných normách, ktoré už boli prevzaté do sústavy STN prekladom.

V časti literatúra sú uvedené slovenské názvy noriem s názvami, ako boli prevzaté prekladom do sústavy STN. Tieto názvy nie bezpodmienečne lícujú s pôvodnými anglickými názvami nových verzií príslušných noriem ISO/IEC.

Vzhľadom na rozsiahlejšiu slovnú zásobu anglického jazyka majú niektoré výrazy viacnásobný význam, resp. ich preklad by v slovenčine mohol byť nezmyselný. Preto je v týchto prípadoch v preklade použitý ten ekvivalent, ktorý je pre kontext vhodnejší, hoc nie je doslovným prekladom pôvodného výrazu.

Základným cieľom tejto medzinárodnej normy je zadefinovať proces zverejňovania zraniteľností od hlásenia až po verejné informovanie o zraniteľnosti a distribúciu opravy. Obsahuje odporúčania pre dodávateľov, ako vytvoriť politiku zverejňovania zraniteľností, aké prvky by malo obsahovať hlásenie o zraniteľnosti a predstavuje základné princípy koordinácie procesu zverejňovania zraniteľností.

Ako pravopisné zdroje boli pri preklade použité Krátky slovník slovenského jazyka a Slovenský národný korpus zo Slovníkového portálu Jazykovedného ústavu Ľ. Štúra SAV, a terminologické databázy, najmä Terminologický portál Jazykovedného ústavu Ľ. Štúra SAV a Terminologická databáza Úradu pre normalizáciu, metrológiu a skúšobníctvo SR.

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) (97 4170)

ISO/IEC 30111 prijatá ako STN EN ISO/IEC 30111 Informačné technológie. Bezpečnostné metódy. Procesy riešenia zraniteľností (ISO/IEC 30111) (97 4189)

Vypracovanie

Spracovateľ: Kompetenčné a certifikačné centrum kybernetickej bezpečnosti, Bratislava
Mgr. Matej Šalmík, PhD.

Technická komisia: TK 37 Informačné technológie

EURÓPSKA NORMA **EN ISO/IEC 29147**
EUROPEAN STANDARD
NORME EUROPÉENNE
EUROPÄISCHE NORM Máj 2020

ICS 35.030

Informačné technológie Bezpečnostné metódy Zverejňovanie zraniteľností (ISO/IEC 29147: 2018)

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

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

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

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 a CENELEC.

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	**CENELEC**
Európsky výbor pre normalizáciu European Committee for Standardization Comité Européen de Normalisation Europäisches Komitee für Normung	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 29147: 2020 SK

Obsah

Contents

Európsky predhovor

Text ISO/IEC 29147: 2018 vypracovala technická komisia ISO/IEC JTC 1 Informačné technológie medzinárodnej organizácie pre normalizáciu (ISO) a bol prevzatý ako EN ISO/IEC 29147: 2020 technickou komisiou CEN/CLC/JTC 13 Kybernetická bezpečnosť a ochrana údajov, 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 29147: 2018 CEN schválil ako EN ISO/IEC 29147: 2020 bez akýchkoľvek modifikácií.

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.

Úvod

V kontexte informačných technológií a kybernetickej bezpečnosti je zraniteľnosť správanie alebo súbor podmienok prítomných v systéme, produkte, komponente alebo službe, ktoré porušujú implicitnú alebo explicitnú bezpečnostnú politiku. Zraniteľnosť možno považovať za slabosť alebo expozíciu, ktorá umožňuje bezpečnostný dopad alebo následok. Útočníci využívajú zraniteľnosti na kompromitáciu dôvernosti, integrity, dostupnosti, prevádzky alebo niektorej inej bezpečnostnej vlastnosti.

Zraniteľnosti často vychádzajú z nedostatkov programu alebo systému pri bezpečnom spracovaní nedôveryhodného alebo neočakávaného vstupu. Medzi príčiny zraniteľnosti patria chyby v kódovaní alebo konfigurácii, prehliadnutia pri voľbe dizajnu a nezabezpečené špecifikácie protokolu a formátu.

Napriek významným snahám zlepšiť bezpečnosť softvéru sú moderné softvéry a systémy také komplexné, že ich vytvorenie bez zraniteľností je nemožné. Faktory rizika zraniteľností zahŕňajú:

- prevádzku a závislosť na systémoch, ktoré majú známe zraniteľnosti;
- nedostatočné informácie o zraniteľnostiach;
- neznalosť existencie zraniteľností.

Tento dokument popisuje zverejňovanie zraniteľností: techniky a politiky pre dodávateľov na prijímanie hlásení o zraniteľnostiach a zverejňovanie informácií o ich odstránení. Zverejňovanie zraniteľností umožňuje nielen odstránenie zraniteľností, ale aj rozhodovanie o rizikách na základe lepších informácií. Zverejňovanie zraniteľností je kritickým prvkom podpory, údržby a prevádzky akéhokoľvek produktu alebo služby, ktorý je vystavený aktívnym hrozbám. Sem patria prakticky všetky produkty alebo služby, ktoré používajú otvorené siete, ako je internet. Schopnosť zverejňovať zraniteľnosti je nevyhnutnou súčasťou vývoja, akvizície, prevádzky a podpory všetkých produktov a služieb. Prevádzka bez schopnosti zverejňovania zraniteľností zvyšuje riziko pre používateľov.

Introduction

In the contexts of information technology and cybersecurity, a vulnerability is a behaviour or set of conditions present in a system, product, component, or service that violates an implicit or explicit security policy. A vulnerability can be thought of as a weakness or exposure that allows a security impact or consequence. Attackers exploit vulnerabilities to compromise confidentiality, integrity, availability, operation, or some other security property.

Vulnerabilities often result from failures of a program or system to securely handle untrusted or unexpected input. Causes that lead to vulnerabilities include errors in coding or configuration, oversights in design choices, and insecure protocol and format specifications.

Despite significant efforts to improve software security, modern software and systems are so complex that it is impractical to produce them without vulnerabilities. Risk factors of vulnerabilities include:

- operating and relying on systems that have known vulnerabilities;
- not having sufficient information about vulnerabilities;
- not knowing that vulnerabilities exist.

This document describes vulnerability disclosure: techniques and policies for vendors to receive vulnerability reports and publish remediation information. Vulnerability disclosure enables both the remediation of vulnerabilities and better-informed risk decisions. Vulnerability disclosure is a critical element of the support, maintenance, and operation of any product or service that is exposed to active threats. This includes practically any product or service that uses open networks such as the Internet. A vulnerability disclosure capability is an essential part of the development, acquisition, operation, and support of all products and services. Operating without vulnerability disclosure capability puts users at increased risk.

Termín „zverejňovanie zraniteľností“ sa používa na opis celkových aktivít spojených s prijímaním hlásení o zraniteľnostiach a poskytovaním informácií o ich odstránení. Ďalšie aktivity, ako je vyšetrovanie a prioritizácia hlásení, vypracovanie, testovanie a nasadenie opatrení na odstránenie zraniteľností a zlepšovanie bezpečného vývoja, sa nazývajú „riešenie zraniteľností“ a sú popísané v ISO/IEC 30111. Termín „zverejnenie“ sa používa aj vo väčšom zmysle pre označenie informovania dotknutej strany o zraniteľnosti po prvýkrát (pozri 3.2).

Hlavné ciele zverejňovania zraniteľností zahŕňajú:

- znižovanie rizika prostredníctvom odstraňovania zraniteľností a informovania používateľov;
- minimalizovanie škody a nákladov spojených so zverejnením;
- poskytovanie dostatočných informácií používateľom pre posúdenie rizika v dôsledku zraniteľností;
- stanovovanie očakávaní s cieľom uľahčiť spoluprácu a koordináciu medzi zainteresovanými stranami.

Procesy popísané v tomto dokumente majú za cieľ minimalizovať riziko, náklady a škody pre všetky zúčastnené strany. Vzhľadom na objem nahlásených zraniteľností, nedostatok presných a úplných informácií a ďalšie faktory je nemožné vytvoriť jednotný, pevný proces, ktorý by sa vzťahoval na každý prípad zverejňovania zraniteľností.

Normatívne prvky v tomto dokumente poskytujú minimálne požiadavky na vytvorenie funkčnej spôsobilosti zverejňovania zraniteľností. Dodávatelia by mali prispôsobiť dodatočné informačné usmernenia v tomto dokumente svojim konkrétnym potrebám a potrebám používateľov a ďalších zúčastnených strán.

The term “vulnerability disclosure” is used to describe the overall activities associated with receiving vulnerability reports and providing remediation information. Additional activities such as investigating and prioritizing reports, developing, testing, and deploying remediations, and improving secure development are called “vulnerability handling” and are described in ISO/IEC 30111. The term “disclosure” is also used more narrowly to mean the act of informing a party about a vulnerability for the first time (see 3.2).

Major goals of vulnerability disclosure include:

- reducing risk by remediating vulnerabilities and informing users;
- minimizing harm and cost associated with the disclosure;
- providing users with sufficient information to evaluate risk due to vulnerabilities;
- setting expectations to facilitate cooperative interaction and coordination among stakeholders.

The processes described in this document aim to minimize risk, cost, and harm to all stakeholders. Due to the volume of reported vulnerabilities, lack of accurate and complete information, and other factors involved, it is not possible to create a single, fixed process that applies to every disclosure event.

The normative elements in this document provide minimum requirements to create a functional vulnerability disclosure capability. Vendors should adapt the additional informative guidance in this document to fit their particular needs and those of users and other stakeholders.

1 Predmet

Tento dokument poskytuje požiadavky a odporúčania dodávateľom týkajúce sa zverejňovania zraniteľností pri svojich produktoch a službách. Zverejňovanie zraniteľností umožňuje používateľom vykonávať technické riadenie zraniteľností, ako je uvedené v norme ISO/IEC 27002: 2013, 12.6.1 [1]. Zverejňovanie zraniteľností pomáha používateľom chrániť svoje systémy a dáta, prioritizovať investície do obrany a lepšie posúdiť riziká. Cieľom zverejňovania zraniteľností je znížiť riziko spojené s využívaním zraniteľností. Koordinované zverejňovanie zraniteľností je obzvlášť dôležité, keď sú dotknutí viacerí dodávatelia. Tento dokument poskytuje:

- usmernenia pre prijímanie hlásení o potenciálnych zraniteľnostiach;
- usmernenia pre zverejňovanie informácií o odstránení zraniteľností;
- termíny a definície, ktoré sú špecifické pre zverejňovanie zraniteľností;
- prehľad konceptov zverejňovania zraniteľností;
- techniky a zohľadnenie politík zverejňovania zraniteľností;
- príklady techník, politík (príloha A) a komunikácie (príloha B).

Ďalšie súvisiace aktivity, ktoré prebiehajú medzi prijatím a zverejnením hlásení o zraniteľnostiach, sú popísané v norme ISO/IEC 30111.

Tento dokument sa vzťahuje na dodávateľov, ktorí sa rozhodnú praktizovať zverejňovanie zraniteľností s cieľom znížiť riziko pre používateľov ich produktov a služieb.

1 Scope

This document provides requirements and recommendations to vendors on the disclosure of vulnerabilities in products and services. Vulnerability disclosure enables users to perform technical vulnerability management as specified in ISO/IEC 27002: 2013, 12.6.1 [1]. Vulnerability disclosure helps users protect their systems and data, prioritize defensive investments, and better assess risk. The goal of vulnerability disclosure is to reduce the risk associated with exploiting vulnerabilities. Coordinated vulnerability disclosure is especially important when multiple vendors are affected. This document provides:

- guidelines on receiving reports about potential vulnerabilities;
- guidelines on disclosing vulnerability remediation information;
- terms and definitions that are specific to vulnerability disclosure;
- an overview of vulnerability disclosure concepts;
- techniques and policy considerations for vulnerability disclosure;
- examples of techniques, policies (Annex A), and communications (Annex B).

Other related activities that take place between receiving and disclosing vulnerability reports are described in ISO/IEC 30111.

This document is applicable to vendors who choose to practice vulnerability disclosure to reduce risk to users of vendors' products and services.

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 všetkých zmien).

ISO/IEC 27000 Informačné technológie. Bezpečnostné metódy. Systémy riadenia informačnej bezpečnosti. Prehľad a slovník

ISO/IEC 30111 Informačné technológie. Bezpečnostné metódy. Procesy riešenia zraniteľností

2 Normative references

The following documents are referred to in the text in such a way that some or all of their content constitutes requirements of this document. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

ISO/IEC 27000 Information technology – Security techniques – Information security management systems – Overview and vocabulary

ISO/IEC 30111 Information technology – Security techniques – Vulnerability handling processes