ČESKÁ TECHNICKÁ NORMA

ICS 35.040 **Březen 2016**

Informační technologie – Bezpečnostní techniky – Postupy zacházení se zranitelnostmi

ČSN
ISO/IEC 30111
36 9706

Information technology – Security techniques – Vulnerability handling processes

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

Tato norma je českou verzí mezinárodní normy ISO/IEC 30111:2013. Překlad byl zajištěn Úřadem pro technickou normalizaci, metrologii a státní zkušebnictví. Má stejný status jako oficiální verze.

This standard is the Czech version of the International Standard ISO/IEC 30111:2013. It was translated by the Czech Office for Standards, Metrology a Testing. It has the same status as the official version.

Národní předmluva

Informace o citovaných dokumentech

ISO/IEC 27000:2014 zavedena v ČSN ISO/IEC 27000:2014 (36 9790) Informační technologie – Bezpečnostní techniky – Systémy řízení bezpečnosti informací – Přehled a slovník

Souvisící ČSN

ČSN ISO/IEC 15408-3 (36 9789) Informační technologie – Bezpečnostní techniky – Kritéria pro hodnocení bezpečnosti IT – Část 3: Komponenty bezpečnostních záruk

ČSN ISO/IEC 27001 (36 9797) Informační technologie – Bezpečnostní techniky – Systémy řízení bezpečnosti informací – Požadavky

ČSN ISO/IEC 27034-1 (36 9703) Informační technologie – Bezpečnostní techniky – Bezpečnost aplikací – Část 1: Přehled a pojmy

Vypracování normy

Zpracovatel: Ing. Alena Hönigová, IČ 61470716

Technická normalizační komise: TNK 20 Informační technologie

Pracovník Úřadu pro technickou normalizaci, metrologii a státní zkušebnictví: Ing. Miroslav Škop

MEZINÁRODNÍ NORMA

Informační technologie – Bezpečnostní techniky – ISO/IEC 30111
Postupy zacházení se zranitelnostmi První vydání
2013-11-01

ICS 35.040

Obsah

Strana

ISO copyright office

Case postale 56 · CH-1211 Geneva 20

Tel. + 41 22 749 01 11

Fax + 41 22 749 09 47

E-mail copyright@iso.org

Web www.iso.org

Published in Switzerland

Předmluva

ISO (Mezinárodní organizace pro normalizaci) a IEC (Mezinárodní elektrotechnická komise) tvoří specializovaný systém celosvětové normalizace. Národní orgány, které jsou členy ISO nebo IEC, se podílejí na vypracování mezi-
národních norem prostřednictvím svých technických komisí ustavených příslušnými organizacemi pro jednotlivé obory technické činnosti. Technické komise ISO a IEC spolupracují v oblastech společných zájmů. Práce se zúčastňují také další vládní a nevládní mezinárodní organizace, s nimiž ISO a IEC navázaly pracovní styk. V oblasti informační technologie zřídily ISO a IEC společnou

technickou komisi ISO/IEC JTC 1.

Návrhy mezinárodních norem jsou vypracovávány v souladu s pravidly danými směrnicemi ISO/IEC, část 2.

Hlavním úkolem společné technické komise je vypracování mezinárodních norem. Návrhy mezinárodních norem přijaté technickými komisemi se rozesílají národním orgánům k hlasování. Vydání mezinárodní normy vyžaduje souhlas alespoň 75 % hlasujících národních orgánů.

Upozorňuje se na možnost, že některé prvky tohoto dokumentu mohou být předmětem patentových práv. ISO a IEC nelze činit odpovědnými za identifikování jakéhokoliv nebo všech patentových práv.

ISO/IEC 30111 vypracovala společná technická komise ISO/IEC JTC 1 *Informační technologie,* subkomise SC 27 *IT Bezpečnostní techniky*.

Úvod

Tato mezinárodní norma popisuje postupy pro prodejce (dodavatele) k zacházení se zprávami o potenciálních zranitelnostech v produktech a online službách.

Tato norma je určena pro spotřebitele, vývojáře, prodejce (dodavatele) a hodnotitele bezpečných IT produktů. Tuto normu mohou dále používat:

- vývojáři a prodejci (dodavatelé), když reagují na ohlášené skutečné nebo potenciální zranitelnosti;
- hodnotitelé, když posuzují bezpečnostní záruku, kterou poskytují postupy pro zacházení se zranitelnostmi prodejců (dodavatelů) a vývojářů a příslušné produkty a služby;
- spotřebitelé, když vybírají produkt a prodejce (dodavatele) online služeb, aby vyjádřili požadavky na záruku vycházející z doporučených postupů vývojářům, prodejcům (dodavatelům) a integrátorům.

Tato mezinárodní norma souvisí s ISO/IEC 29147.[5] Je propojena s prvky popsanými v ISO/IEC 29147 v případě přijímání zpráv o potenciální zranitelnosti a v případě distribuování informací o řešení zranitelností.

Tato mezinárodní norma zohledňuje příslušné prvky ISO/IEC 15408-3,[1] 13.5 Náprava závad (ALC_FLR).

1 Předmět normy

Tato mezinárodní norma obsahuje směrnice, jak postupovat a řešit informace o potenciální zranitelnosti v produktu nebo online službě.

Tato mezinárodní norma je vhodná pro prodejce (dodavatele) zapojené do zacházení se zranitelnostmi.