ČESKÁ TECHNICKÁ NORMA

ICS 35.030 **Květen**
2022

Bezpečnost informací – Kritéria a metodika pro hodnocení bezpečnosti biometrických systémů – Část 2: Výkonnost biometrického rozpoznávání

ČSN
ISO/IEC 19989-2

36 9859

Information security – Criteria and methodology for security evaluation of biometric systems – Part 2: Biometric recognition performance

Sécurité de l,information – Criteres et méthodologie pour l,évaluation de la sécurité des systemes biométriques –
Partie 2: Efficacité de reconnaissance biométrique

Tato norma je českou verzí mezinárodní normy ISO/IEC 19989-2:2020. Překlad byl zajištěn Českou agenturou pro standardizaci. Má stejný status jako oficiální verze.

This standard is the Czech version of the International Standard ISO/IEC 19989-2:2020. It was translated by the Czech Standardization Agency. It has the same status as the official version.

Národní předmluva

Informace o citovaných dokumentech

ISO/IEC 2382:2015 nezavedena1)

ISO/IEC 2382-37:2017 zavedena v ČSN ISO/IEC 2382-37:2018 (36 9001) Informační technologie – Slovník – Část 37: Biometrika

ISO/IEC 15408-1:2009 zavedena v ČSN EN ISO/IEC 15408-1:2013 (36 9789) Informační technologie – Bezpečnostní techniky – Kritéria pro hodnocení bezpečnosti IT – Část 1: Úvod a obecný model

ISO/IEC 15408-3:2008 zavedena v ČSN EN ISO/IEC 15408-3:2010 (36 9789) Informační technologie – Bezpečnostní techniky – Kritéria pro hodnocení bezpečnosti IT – Část 3: Komponenty bezpečnostních záruk

ISO/IEC 18045:2008 zavedena v ČSN EN ISO/IEC 18045:2020 (36 9805) Informační technologie – Bezpečnostní
techniky – Metodika pro hodnocení bezpečnosti IT

ISO/IEC 19792:2009 zavedena v ČSN ISO/IEC 19792:2016 (36 9858) Informační technologie –

Bezpečnostní techniky – Hodnocení bezpečnosti biometriky

ISO/IEC 19795-1:2006 nezavedena2)

ISO/IEC 19795-2:2007 zavedena v ČSN ISO/IEC 19795-2:2009 (36 9861) Informační technologie – Testování a hodnocení výkonnosti biometrik – Část 2: Metodologie testování pro hodnocení technologie a scénáře

ISO/IEC 19989-1:2020 zavedena v ČSN ISO/IEC 19989-1:2021 (36 9859) Bezpečnost informací – Kritéria a metodika pro hodnocení bezpečnosti biometrických systémů – Část 1: Rámec

ISO/IEC 30107-3:2017 zavedena v ČSN ISO/IEC 30107-3:2019 (36 9862) Informační technologie – Detekce
biometrického prezentačního útoku – Část 3: Testování a podávání zpráv

Souvisící ČSN

ČSN ISO/IEC 2382-37:2018 (36 9001) Informační technologie – Slovník – Část 37: Biometrika

ČSN EN ISO/IEC 15408-1:2013 (36 9789) Informační technologie – Bezpečnostní techniky – Kritéria pro hodnocení bezpečnosti IT – Část 1: Úvod a obecný model

ČSN ISO/IEC 30107-1:2019 (36 9862) Informační technologie – Detekce biometrického prezentačního útoku – Část 1: Rámec

ČSN ISO/IEC 30107-3:2019 (36 9862) Informační technologie – Detekce biometrického prezentačního útoku – Část 3: Testování a podávání zpráv

Vypracování normy

Zpracovatel: Prof. Ing., Dipl. Ing. Martin Drahanský, Ph.D., IČO 73840602

Technická normalizační komise: TNK 20 Informační technologie

Pracovník České agentury pro standardizaci: Ing. Miroslav Škop

Česká agentura pro standardizaci je státní příspěvková organizace zřízená Úřadem pro technickou normalizaci, metrologii a státní zkušebnictví na základě ustanovení § 5 odst. 2 zákona č. 22/1997 Sb., o technických požadavcích na výrobky a o změně a doplnění některých zákonů, ve znění pozdějších předpisů.

MEZINÁRODNÍ NORMA

Bezpečnost informací – Kritéria a metodika pro hodnocení bezpečnosti biometrických systémů – Část 2: Výkonnost biometrického rozpoznávání

ISO/IEC 19989-2
První vydání
2020-10

ICS 35.030

Obsah

Strana

Strana

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 mezinárodních norem prostřednictvím svých technických komisí ustavených příslušnými organizacemi pro jednotlivé obory technické činnosti. Technické komise ISO a IEC spolupracují v oborech společného zájmu. Práce se zúčastňují také další vládní i nevládní mezinárodní organizace, s nimiž ISO a IEC navázaly pracovní styk.

Postupy použité při tvorbě tohoto dokumentu a postupy určené pro jeho další udržování jsou popsány ve směrnicích ISO/IEC, část 1. Zejména se má věnovat pozornost rozdílným schvalovacím kritériím potřebným pro různé druhy dokumentů. Tento dokument byl vypracován v souladu s redakčními pravidly uvedenými ve směrnicích ISO/IEC, část 2 (viz www.iso.org/directives).

Upozorňuje se na možnost, že některé prvky tohoto dokumentu mohou být předmětem patentových práv. ISO a IEC nelze činit odpovědnými za identifikaci jakéhokoliv nebo všech patentových práv. Podrobnosti o jakýchkoliv patentových právech identifikovaných během přípravy tohoto dokumentu budou uvedeny v úvodu a/nebo v seznamu patentových prohlášení obdržených ISO (viz www.iso.org/patents) nebo v seznamu patentových prohlášení obdržených IEC (viz http://patents.iec.ch).

Jakýkoliv obchodní název použitý v tomto dokumentu se uvádí jako informace pro usnadnění práce uživatelů a neznamená schválení.

Vysvětlení nezávazného charakteru technických norem, významu specifických termínů a výrazů ISO, které se vztahují k posuzování shody, jakož i informace o tom, jak ISO dodržuje principy Světové obchodní organizace (WTO) týkající se technických překážek obchodu (TBT), jsou uvedeny na www.iso.org/iso/foreword.html.

Tento dokument vypracovala společná technická komise ISO/IEC JTC 1 *Informační technologie*, subkomise SC 27 *Bezpečnost informací, kybernetická bezpečnost a ochrana soukromí*.

Seznam všech částí souboru ISO/IEC 19989 lze nalézt na webových stránkách ISO.

Jakákoli zpětná vazba nebo otázky týkající se tohoto dokumentu mají být adresovány národnímu normalizačnímu orgánu uživatele. Úplný seznam těchto orgánů lze nalézt na adrese www.iso.org/members.html.

Úvod

Biometrické systémy mohou být zranitelné vůči prezentačním útokům, kdy se útočníci pokoušejí rozvrátit bezpečnostní politiku systému tím, že prezentují své přirozené biometrické charakteristiky nebo artefakty obsahující
kopírované nebo předstírané vlastnosti. K prezentačním útokům může dojít během událostí registrace nebo identifikace/ověření. Techniky určené k detekci prezentačních artefaktů se obecně liší od technik odvrácení útoků, kde se používají přirozené charakteristiky. Ochrana před prezentačními útoky s přirozenými charakteristikami se obvykle spoléhá na schopnost biometrického systému rozlišovat mezi oprávněnými registrovanými subjekty a útočníky na základě rozdílů mezi jejich přirozenými biometrickými charakteristikami. Tato schopnost je charakterizována výkonností biometrického rozpoznávání systému – jak dobře nebo špatně vykonává systém biometrického rozpoznávání požadované funkce. Výkonnost biometrického rozpoznávání a detekce prezentačního útoku mají vliv na bezpečnost biometrických systémů. Hodnocení těchto aspektů výkonnosti z hlediska bezpečnosti se proto stane důležitým faktorem při pořizování biometrických produktů a systémů.

Biometrické produkty a systémy sdílejí mnoho vlastností jiných produktů a systémů IT, u kterých se k hodnocení bezpečnosti z pohledu normalizace využívá soubor ISO/IEC 15408 a ISO/IEC 18045. Biometrické systémy však ztělesňují určité funkce, které vyžadují specializovaná hodnotící kritéria a metodiku, která nejsou řešena v souboru ISO/IEC 15408 ani v ISO/IEC 18045. Tyto se týkají především hodnocení biometrického rozpoznávání a detekce prezentačního útoku. To jsou funkce, kterým se věnuje soubor ISO/IEC 19989.

ISO/IEC 19792 popisuje tyto biometrické aspekty a specifikuje principy, které je třeba vzít v úvahu při hodnocení bezpečnosti biometrických systémů. Nespecifikuje však konkrétní kritéria a metodiku, které jsou nutné pro hodnocení bezpečnosti na základě souboru ISO/IEC 15408.

Soubor ISO/IEC 19989 představuje most mezi principy hodnocení biometrických produktů a systémů definovaných v ISO/IEC 19792 a kritérii a metodickými požadavky pro hodnocení bezpečnosti na základě souboru ISO/IEC 15408. Soubor ISO/IEC 19989 doplňuje soubor ISO/IEC 15408 a ISO/IEC 18045 tím, že poskytuje rozšířené bezpečnostní funkční požadavky spolu s činnostmi záruk souvisícími s těmito požadavky. Rozšíření požadavků a činnostmi záruk nalezených v souboru ISO/IEC 15408
a v ISO/IEC 18045 souvisí s hodnocením biometrického rozpoznávání a detekcí prezentačního útoku, které se týkají zejména biometrických systémů.

ISO/IEC 19989-1 spočívá v zavedení obecného rámce pro hodnocení bezpečnosti biometrických systémů, včetně rozšířených bezpečnostních funkčních komponent, a doplňkové metodiky, což jsou další činnosti hodnocení pro hodnotitele. Podrobná doporučení jsou pro aspekty výkonnosti biometrického rozpoznávání vypracovány v tomto dokumentu a pro aspekty detekce prezentačního útoku v ISO/IEC 19989-3.

Tento dokument popisuje doplňky k metodice hodnocení pro hodnocení výkonnosti biometrického rozpoznávání pro hodnocení bezpečnosti biometrických produktů. Doplňuje soubor ISO/IEC 15408, ISO/IEC 18045 a ISO/IEC 19989-1. Navazuje na obecné úvahy popsané v ISO/IEC 19792 a na metodiku testování biometrické výkonnosti popsanou v ISO/IEC 19795-1 tím, že hodnotiteli poskytuje další návod.

Zatímco se v ISO/IEC 19989-1 používá termín „uživatel“, v tomto dokumentu se používá „subjekt údajů“, aby byl v souladu s biometrickým slovníkem, protože hlavními čtenáři tohoto dokumentu by měli být odborníci na biometriku.

1 Předmět normy

Pro hodnocení bezpečnosti systémů biometrického ověření a systémů biometrické identifikace se tento dokument věnuje bezpečnostnímu hodnocení výkonnosti biometrického rozpoznávání podle souboru ISO/IEC 15408.

Poskytuje vývojáři a hodnotiteli požadavky a doporučení pro doplňkové činnosti týkající se výkonnosti biometrického rozpoznávání specifikované v ISO/IEC 19989-1.

Hodnocení technik detekce prezentačních útoků je mimo rozsah tohoto dokumentu, s výjimkou prezentace pokusů podvodníka podle zásad zamýšleného použití podle dokumentační příručky TOE.

---

1) ISO/IEC 2382:2015 je volně dostupná na adrese http://www.iso.org/obp.

2) ČSN ISO/IEC 19795-1:2008, která přejímala ISO/IEC 19795-1:2006, byla zrušena z důvodu nahrazení mezinárodní normy novějším vydáním a je dostupná v zákaznickém centru ČAS.