Uradni list
Evropske unije

SL
Serija L

2024/3144

19.12.2024

IZVEDBENA UREDBA KOMISIJE (EU) 2024/3144

z dne 18. decembra 2024

o spremembi Izvedbene uredbe (EU) 2024/482 v zvezi z veljavnimi mednarodnimi standardi in popravku navedene izvedbene uredbe

(Besedilo velja za EGP)

EVROPSKA KOMISIJA JE –

ob upoštevanju Pogodbe o delovanju Evropske unije,

ob upoštevanju Uredbe (EU) 2019/881 Evropskega parlamenta in Sveta z dne 17. aprila 2019 o Agenciji Evropske unije za kibernetsko varnost (Agencija ENISA) in o certificiranju informacijske in komunikacijske tehnologije na področju kibernetske varnosti ter razveljavitvi Uredbe (EU) št. 526/2013 (Akt o kibernetski varnosti) ([1]) in zlasti člena 49(7) Uredbe,

ob upoštevanju naslednjega:

(1) Izvedbena uredba Komisije (EU) 2024/482 ([2]) določa vloge, pravila in obveznosti ter strukturo evropske certifikacijske sheme za kibernetsko varnost, ki temelji na skupnih merilih (v nadaljnjem besedilu: EUCC) v skladu z evropskim certifikacijskim okvirom za kibernetsko varnost iz Uredbe (EU) 2019/881.

(2) Izvedbena uredba (EU) 2024/482 temelji na uveljavljenih mednarodnih standardih, in sicer skupnih merilih in skupni metodologiji ocenjevanja, ki jih vzdržujeta Mednarodna organizacija za standardizacijo (ISO) in Mednarodna elektrotehniška komisija (IEC). Izvedbena uredba (EU) 2024/482 se sklicuje na standarde ISO/IEC, vendar ne določa veljavne različice navedenih standardov. Zato bi bilo treba določiti, katera različica standardov se uporablja za certifikate, izdane na podlagi EUCC.

(3) Vladne organizacije, ki so prispevale k razvoju skupnih meril in skupne metodologije ocenjevanja z dogovorom o priznavanju certifikatov na podlagi skupnih meril na področju varnosti IT so skupni imetniki, skupaj z ISO/IEC avtorskih pravic zanje. Navedene vladne organizacije ohranijo pravico do njihove uporabe. Glede na pomen teh dokumentov, ki temeljijo na dogovoru o priznavanju certifikatov na podlagi skupnih meril, bi morali biti tudi podlaga za certificiranje na podlagi EUCC.

(4) Standardi v zvezi s skupnimi merili in skupno metodologijo ocenjevanja so predmet razlag v okviru dogovora o priznavanju certifikatov na podlagi skupnih meril, ki olajšujejo njihovo izvajanje in jih lahko upoštevajo centri za ocenjevanje varnosti informacijske tehnologije in certifikacijski organi.

(5) Mednarodni standardi, povezani s skupnimi merili, se lahko posodobijo. Za zagotovitev urejenega in pravočasnega prehoda je primerno opredeliti prehodna pravila, da se prodajalcem, centrom za ocenjevanje varnosti informacijske tehnologije in certifikacijskim organom ter drugim ustreznim akterjem zagotovi dovolj časa za potrebne prilagoditve. Taka prehodna pravila bi morala biti v ustrezni meri usklajena z globalnimi praksami, kot so prakse, ki jih določa dogovor o priznavanju certifikatov na podlagi skupnih meril.

([1]) UL L 151, 7.6.2019, str. 15, ELI: http://data.europa.eu/eli/reg/2019/881/oj.
([2]) Izvedbena uredba Komisije (EU) 2024/482 z dne 31. januarja 2024 o določitvi pravil za uporabo Uredbe (EU) 2019/881 Evropskega parlamenta in Sveta v zvezi s sprejetjem evropske certifikacijske sheme za kibernetsko varnost, ki temelji na skupnih merilih (UL L, 2024/482, 7.2.2024, ELI: http://data.europa.eu/eli/reg_impl/2024/482/oj).

(6) Izvedbena uredba (EU) 2024/482 ne določa podrobno, do kdaj lahko certifikacija proizvoda IKT temelji na predhodnih različicah standardov v zvezi s skupnimi merili in skupno metodologijo ocenjevanja. Tehnična področja in profili zaščite, navedeni v prilogah I, II in III k navedeni izvedbeni uredbi, temeljijo na prejšnjih različicah standardov ISO/IEC 15408 in 18045. Izvedbena uredba (EU) 2024/482 bi zato morala podrobno določati, v katerih okoliščinah se prejšnja različica skupnih meril in skupne metodologije ocenjevanja še vedno uporablja in kako bo potekal prehod na najnovejšo različico mednarodnih standardov.

(7) V prehodnem obdobju bi morala biti prednostna naloga ustreznih deležnikov, da se posodobijo ustrezna tehnična področja in profili zaščite. Izvedbena uredba (EU) 2024/482 bi morala določati, da bodo varnostni cilji, ki temeljijo na prejšnji različici standardov, sprejeti do 31. decembra 2027 v skladu s prehodno politiko, ki je bila sprejeta z dogovorom o priznavanju certifikatov na podlagi skupnih meril. Vendar je treba opozoriti, da prehodna politika v zvezi z dogovorom o priznavanju certifikatov na podlagi skupnih meril zajema prvotne ocene proizvodov in profilov zaščite z datumom najpozneje 30. junija 2024, ko se EUCC še ni uporabljala. Poleg tega bi morala Izvedbena uredba (EU) 2024/482 v skladu s prehodno politiko v zvezi z dogovorom o priznavanju certifikatov na podlagi skupnih meril določati, da bodo varnostni cilji, skladni z navedeno izvedbeno uredbo, ki potrjuje skladnost s profili zaščite na podlagi prejšnje različice standardov, sprejeti do 31. decembra 2027. Poleg tega bi moralo biti mogoče uporabiti prejšnjo različico standardov, kadar se na podlagi Izvedbene uredbe (EU) 2024/482 izda nov certifikat v okviru postopka pregleda nacionalnega certifikata, ki se začne v dveh letih od izdaje prvotnega certifikata. To ne bi bilo relevantno za postopek pregleda, ki ne zahteva izdaje novega certifikata v skladu z Izvedbeno uredbo (EU) 2024/482 in pri katerem certifikat ostane veljaven.

(8) Za zagotovitev urejenega prehoda na najnovejšo različico standardov bi morala Izvedbena uredba (EU) 2024/482 določati posebna prehodna pravila in še naprej omogočati izdajo certifikatov na podlagi navedene izvedbene uredbe, ki potrjuje skladnost s profili zaščite na podlagi prejšnjih različic standardov, ki so bili objavljeni na podlagi dogovora o priznavanju certifikatov na podlagi skupnih meril, kadar se uporaba takih profilov zaščite zahteva v skladu z zakonodajo Unije. To velja za Izvedbeno uredbo Komisije (EU) 2016/799 ([3]) in Uredbo (EU) št. 910/2014 Evropskega parlamenta in Sveta ([4]) ter Izvedbeni sklep Komisije (EU) 2016/650 ([5]).

(9) V Prilogi I k Izvedbeni uredbi (EU) 2024/482 so navedeni veljavni najsodobnejši dokumenti za ocenjevanje proizvodov IKT in profilov zaščite. Vendar pa v njej ni podrobno določena različica dokumentov. Zato bi bilo treba določiti, katera različica dokumentov se uporablja za certifikate, izdane na podlagi EUCC. Te različice temeljijo na dokumentih, ki jih je potrdila evropska certifikacijska skupina za kibernetsko varnost, pri čemer je bil opravljen nadaljnji pregled njihove vključitve v EUCC. Poleg tega bi bilo treba Prilogo I spremeniti, da se vključijo posodobljeni in novi najsodobnejši dokumenti, potem ko jih potrdi evropska certifikacijska skupina za kibernetsko varnost, s čimer se zagotovi enotna akreditacija organov za ugotavljanje skladnosti na podlagi EUCC. Zahteve za akreditacijo centrov za ocenjevanje varnosti informacijske tehnologije bi bilo treba posodobiti, da se pojasni uporaba meril neodvisnosti in nepristranskosti, za akreditacijo certifikacijskih organov pa bi bilo treba določiti nov najsodobnejši dokument.

(10) Najsodobnejši dokumenti se lahko dodajo v EUCC ali se posodobijo v okviru dejavnosti vzdrževanja EUCC. Za nove ali posodobljene najsodobnejše dokumente bo morda treba določiti ustrezna prehodna pravila, ki bodo prodajalcem, centrom za ocenjevanje varnosti informacijske tehnologije, certifikacijskim organom in drugim deležnikom omogočala potrebne prilagoditve. Za posodobitev najsodobnejšega dokumenta v zvezi z akreditacijo centrov za ocenjevanje varnosti informacijske tehnologije bi se moral za akreditacije, izdane pred 8. julijem 2025, posodobljeni dokument uporabljati le pri njihovem pregledu, na primer v okviru postopka ocenjevanja ali ponovnega ocenjevanja. Poleg tega bi se moral posodobljeni dokument uporabljati za vse akreditacije za centre za ocenjevanje varnosti informacijske tehnologije, izdane po 8. juliju 2025.

([3]) Izvedbena uredba Komisije (EU) 2016/799 z dne 18. marca 2016 o izvajanju Uredbe (EU) št. 165/2014 Evropskega parlamenta in Sveta za določitev zahtev glede konstrukcije, preskušanja, namestitve, delovanja in popravila tahografov in njihovih sestavnih delov (UL L 139, 26.5.2016, str. 1, ELI: http://data.europa.eu/eli/reg_impl/2016/799/oj).

([4]) Uredba (EU) št. 910/2014 Evropskega parlamenta in Sveta z dne 23. julija 2014 o elektronski identifikaciji in storitvah zaupanja za elektronske transakcije na notranjem trgu in o razveljavitvi Direktive 1999/93/ES (UL L 257, 28.8.2014, str. 73, ELI: http://data.europa.eu/eli/reg/2014/910/oj).

([5]) Izvedbeni sklep Komisije (EU) 2016/650 z dne 25. aprila 2016 o določitvi standardov za oceno varnosti naprav za ustvarjanje kvalificiranega elektronskega podpisa in žiga v skladu s členoma 30(3) in 39(2) Uredbe (EU) št. 910/2014 Evropskega parlamenta in Sveta o elektronski identifikaciji in storitvah zaupanja za elektronske transakcije na notranjem trgu (UL L 109, 26.4.2016, str. 40, ELI: http://data.europa.eu/eli/dec_impl/2016/650/oj).

(11) Dodatni popravki členov 5, 8, 16, 29 in 44 ter Priloge IV Izvedbene uredbe (EU) 2024/482 prispevajo k zagotavljanju enotne in jasne pravne razlage.

(12) Pravila o priglasitvah organov za ugotavljanje skladnosti bi bilo treba določiti horizontalno za vse sheme na podlagi evropskega certifikacijskega okvira za kibernetsko varnost. Izvedbena uredba Komisije (EU) 2024/3143 ([6]) zajema taka pravila o priglasitvi. Zato bi bilo treba črtati člena 23 in 24 Izvedbene uredbe (EU) 2024/482 z dnem začetka veljavnosti Izvedbene uredbe 2024/3143.

(13) Izvedbeno uredbo (EU) 2024/482 bi bilo zato treba ustrezno spremeniti in popraviti.

(14) Ukrepi iz te uredbe so v skladu z mnenjem odbora, ustanovljenega s členom 66 Uredbe (EU) 2019/881 –

SPREJELA NASLEDNJO UREDBO:

Člen 1

Izvedbena uredba (EU) 2024/482 se spremeni:

(1) v členu 2 se točki 1 in 2 nadomestita z naslednjim:

„(1) ‚skupna merila‘ pomeni skupna merila za ocenjevanje varnosti informacijske tehnologije, kot so določena v standardih ISO/IEC 15408-1:2022, ISO/IEC 15408-2:2022, ISO/IEC 15408-3:2022, ISO/IEC 15408-4:2022 ali ISO/IEC 15408-5:2022 ali določena v skupnih merilih za ocenjevanje varnosti informacijske tehnologije, različica CC:2022, deli 1 do 5, ki so jih objavili udeleženci dogovora o priznavanju certifikatov na podlagi skupnih meril na področju varnosti IT;

(2) ‚skupna metodologija ocenjevanja‘ pomeni skupno metodologijo za ocenjevanje varnosti informacijske tehnologije, kot je določena v standardu ISO/IEC 18045:2022, ali skupno metodologijo za ocenjevanje varnosti informacijske tehnologije, različica CEM:2022, ki so jo objavili udeleženci dogovora o priznavanju certifikatov na podlagi skupnih meril na področju varnosti IT;“;

(2) člen 3 se nadomesti z naslednjim:

„*Člen 3*

Standardi ocenjevanja

1. Pri ocenjevanjih, izvedenih v okviru EUCC, veljajo naslednji standardi:

(a) skupna merila in

(b) skupna metodologija ocenjevanja.

2. Do 31. decembra 2027 se lahko izda certifikat na podlagi EUCC, ki uporablja enega od naslednjih standardov:

(a) ISO/IEC 15408-1:2009, ISO/IEC 15408-2:2008 ali ISO/IEC 15408-3:2008;

(b) skupna merila za ocenjevanje varnosti informacijske tehnologije, različica 3.1, revizija 5, ki so jih objavili udeleženci dogovora o priznavanju certifikatov na podlagi skupnih meril na področju varnosti IT;

([6]) Izvedbena uredba Komisije (EU) 2024/3143 z dne 18. decembra 2024 o določitvi okoliščin, oblik in postopkov za priglasitve v skladu s členom 61(5) Uredbe (EU) 2019/881 Evropskega parlamenta in Sveta o Agenciji Evropske unije za kibernetsko varnost (ENISA) in o certificiranju informacijske in komunikacijske tehnologije na področju kibernetske varnosti (UL L, 2024/3143, 19.12.2024, ELI: http://data.europa.eu/eli/reg_impl/2024/3143/oj).

(c) ISO/IEC 18045:2008;

(d) skupna metodologija za ocenjevanje varnosti informacijske tehnologije, revizija 5, različica 3.1, ki so jo objavili udeleženci dogovora o priznavanju certifikatov na podlagi skupnih meril na področju varnosti IT.

3. Do 31. decembra 2027 se lahko izda certifikat na podlagi EUCC, ki uporablja standarde iz odstavka 1 in ki potrjuje skladnost s profilom zaščite, ki uporablja standarde iz odstavka 2.

4. Certifikat, s katerim se uporabljajo standardi iz odstavka 1, se lahko izda na podlagi EUCC, ki potrjuje skladnost s profilom zaščite, ki uporablja katerega koli od naslednjih standardov, če uporabo takega profila zaščite zahteva Izvedbena uredba Komisije (EU) 2016/799 (*), Uredba (EU) št. 910/2014 Evropskega parlamenta in Sveta (**) ali Izvedbeni sklep Komisije (EU) 2016/650 (***):

(a) skupna merila za ocenjevanje varnosti informacijske tehnologije, različica 3.1, revizije 1 do 4, ki so jih objavili udeleženci dogovora o priznavanju certifikatov na podlagi skupnih meril na področju varnosti IT;

(b) skupna metodologija za ocenjevanje varnosti informacijske tehnologije, različica 3.1, revizije 1 do 4, ki so jo objavili udeleženci dogovora o priznavanju certifikatov na podlagi skupnih meril na področju varnosti IT.

_____

(*) Izvedbena uredba Komisije (EU) 2016/799 z dne 18. marca 2016 o izvajanju Uredbe (EU) št. 165/2014 Evropskega parlamenta in Sveta za določitev zahtev glede konstrukcije, preskušanja, namestitve, delovanja in popravila tahografov in njihovih sestavnih delov (UL L 139, 26.5.2016, str. 1, ELI: http://data.europa.eu/eli/reg_impl/2016/799/oj).

(**) Uredba (EU) št. 910/2014 Evropskega parlamenta in Sveta z dne 23. julija 2014 o elektronski identifikaciji in storitvah zaupanja za elektronske transakcije na notranjem trgu in o razveljavitvi Direktive 1999/93/ES (UL L 257, 28.8.2014, str. 73, ELI: http://data.europa.eu/eli/reg/2014/910/oj).

(***) Izvedbeni sklep Komisije (EU) 2016/650 z dne 25. aprila 2016 o določitvi standardov za oceno varnosti naprav za ustvarjanje kvalificiranega elektronskega podpisa in žiga v skladu s členoma 30(3) in 39(2) Uredbe (EU) št. 910/2014 Evropskega parlamenta in Sveta o elektronski identifikaciji in storitvah zaupanja za elektronske transakcije na notranjem trgu (UL L 109, 26.4.2016, str. 40, ELI: http://data.europa.eu/eli/dec_impl/2016/650/oj).“;

(3) v poglavju IV se vstavi naslednji člen 20a:

„*Člen 20a*

Specifikacija zahtev za akreditacijo organov za ugotavljanje skladnosti

Pri akreditaciji organov za ugotavljanje skladnosti se upošteva specifikacija zahtev za akreditacijo certifikacijskih organov in centrov za ocenjevanje varnosti informacijske tehnologije, kot je določeno v veljavnih najsodobnejših dokumentih iz točke 2 Priloge I.“;

(4) člena 23 in 24 se črtata;

(5) v členu 48 se doda naslednji odstavek 4:

„4. Če v Prilogi I ali II ni določeno drugače, se najsodobnejši dokumenti uporabljajo od datuma začetka uporabe akta o spremembi, s katerim so bili vključeni v Prilogo I ali II.“;

(6) v členu 49 se doda naslednji odstavek 4:

„4. Pri izvajanju pregleda iz odstavka 3 v dveh letih od izdaje prvotnega certifikata in kadar se zaradi takega pregleda izda nov certifikat v skladu s to uredbo, se lahko uporabijo standardi iz člena 3(2). Datum izdaje prvotnega certifikata se razume kot datum izdaje zadnjega certifikata za proizvod IKT ali profil zaščite, na katerem temelji sedanje certificiranje.“;

(7) Priloga I se nadomesti z besedilom iz Priloge I k tej uredbi;

(8) Priloga IV se spremeni v skladu s Prilogo II k tej uredbi.

Člen 2

Izvedbena uredba (EU) 2024/482 se popravi:

(1) v členu 5(1) se točka (b) nadomesti z naslednjim:

„(b) z navajanjem skladnosti s certificiranim profilom zaščite kot dela postopka IKT, kadar proizvod IKT spada v kategorijo proizvodov IKT, ki jo zajema navedeni profil zaščite.“;

(2) člen 8 se popravi:

(a) naslov se nadomesti z naslednjim:

„Informacije, ki so potrebne za certificiranje in ocenjevanje“;

(b) odstavek 1 se nadomesti z naslednjim:

„1. Vložnik za certificiranje v okviru EUCC certifikacijskemu organu in centru za ocenjevanje varnosti informacijske tehnologije zagotovi ali da drugače na voljo vse potrebne informacije za dejavnosti certificiranja in ocenjevanja.“;

(3) člen 16 se nadomesti z naslednjim:

„*Člen 16*

Informacije, potrebne za certificiranje in oceno profilov zaščite

Vložnik za certificiranje profila zaščite certifikacijskemu organu in centru za ocenjevanje varnosti informacijske tehnologije zagotovi ali da drugače na voljo vse potrebne informacije v popolni in pravilni obliki za dejavnosti certificiranja in ocenjevanja. Smiselno se uporablja člen 8(2), (3), (4) in (7).“;

(4) v členu 17 se črta odstavek 1;

(5) v členu 29 se odstavek 2 nadomesti z naslednjim:

„2. Če imetnik certifikata EUCC v roku iz odstavka 1 ne predlaga ustreznega popravnega ukrepa, se certifikat začasno prekliče v skladu s členom 30 ali odvzame v skladu s členoma 14 ali 20.“.

Člen 3

Ta uredba začne veljati dvajseti dan po objavi v *Uradnem listu Evropske unije*.

Člen 1(4) se uporablja od 8. januarja 2025.

Ta uredba je v celoti zavezujoča in se neposredno uporablja v vseh državah članicah.

V Bruslju, 18. decembra 2024

Za Komisijo
predsednica
Ursula VON DER LEYEN

PRILOGA I

„„PRILOGA I

Najsodobnejši dokumenti za tehnična področja in drugi najsodobnejši dokumenti

1. Najsodobnejši dokumenti za tehnična področja na ravni 4 ali 5 AVA_VAN:

   (a) naslednji dokumenti, povezani s harmoniziranim ocenjevanjem tehnične domene ‚Pametne kartice in podobne naprave‘:

      (1) ‚Minimalne zahteve centra za ocenjevanje varnosti informacijske tehnologije za ocenjevanje varnosti pametnih kartic in podobnih naprav‘, različica 1.1;

      (2) ‚Minimalne varnostne zahteve za lokacijo‘, različica 1.1;

      (3) ‚Uporaba skupnih meril za integrirana vezja‘, različica 1.1;

      (4) ‚Zahteve za varnostno arhitekturo (ADV_ARC) pametnih kartic in podobnih naprav‘, različica 1.1;

      (5) ‚Certificiranje ‚odprtih‘ proizvodov za pametne kartice‘, različica 1.1;

      (6) ‚Ocenjevanje sestavljenih proizvodov za pametne kartice in podobne naprave‘, različica 1.1;

      (7) ‚Uporaba potenciala napada na pametne kartice in podobne naprave‘, različica 1.2;

   (b) naslednji dokumenti, povezani s harmoniziranim ocenjevanjem tehnične domene ‚Naprave strojne opreme z varnostnimi napravami‘:

      (1) ‚Minimalne zahteve centra za ocenjevanje varnosti informacijske tehnologije za ocenjevanje varnosti naprav strojne opreme z varnostnimi napravami‘, različica 1.1;

      (2) ‚Minimalne varnostne zahteve za lokacijo‘, različica 1.1;

      (3) ‚Uporaba potenciala napada na naprave strojne opreme z varnostnimi napravami‘, različica 1.2.

2. Najsodobnejši dokumenti, povezani s harmonizirano akreditacijo organov za ugotavljanje skladnosti:

   (a) ‚Akreditacija centrov za ocenjevanje varnosti informacijske tehnologije za EUCC‘, različica 1.1, za akreditacije, izdane pred 8. julijem 2025;

   (b) ‚Akreditacija centrov za ocenjevanje varnosti informacijske tehnologije za EUCC‘, različica 1.6c, za akreditacije, izdane prvič ali pregledane po 8. juliju 2025;

   (c) ‚Akreditacija certifikacijskih organov za EUCC‘, različica 1.6b.“.“.

PRILOGA II

V Prilogi IV, oddelek IV.3, k Izvedbeni uredbi (EU) 2024/482 se točki 5 in 6 nadomestita z naslednjim:

„5. Če certifikacijski organ potrdi, da so spremembe manjše, se za spremenjeni proizvod IKT ne izda nov certifikat in se pripravi poročilo o vzdrževanju k prvotnemu poročilu o certificiranju.

Poročilo o vzdrževanju se vključi kot del poročila o analizi učinka posledic in vsebuje naslednje oddelke:

(a) uvod,

(b) opis sprememb,

(c) dokaz o razvijalcu, na katerega to vpliva.

6. Novo poročilo o vzdrževanju iz točke 5 se pošlje Agenciji ENISA za objavo na spletišču o certificiranju na področju kibernetske varnosti.“.