2024/3144

19.12.2024.

PROVEDBENA UREDBA KOMISIJE (EU) 2024/3144

od 18. prosinca 2024.

o izmjeni Provedbene uredbe (EU) 2024/482 u pogledu primjenjivih međunarodnih normi i o ispravku te provedbene uredbe

(Tekst značajan za EGP)

EUROPSKA KOMISIJA,

uzimajući u obzir Ugovor o funkcioniranju Europske unije,

uzimajući u obzir Uredbu (EU) 2019/881 Europskog parlamenta i Vijeća od 17. travnja 2019. o ENISA-i (Agencija Europske unije za kibersigurnost) te o kibersigurnosnoj certifikaciji u području informacijske i komunikacijske tehnologije i stavljanju izvan snage Uredbe (EU) br. 526/2013 (Akt o kibersigurnosti) ([1]), a posebno njezin članak 49. stavak 7.,

budući da:

(1) Provedbenom uredbom Komisije (EU) 2024/482 ([2]) utvrđuju se uloge, pravila i obveze i struktura europskog programa kibernetičkosigurnosne certifikacije na temelju zajedničkih kriterija (EUCC) u skladu s europskim okvirom za kibernetičkosigurnosnu certifikaciju utvrđenim u Uredbi (EU) 2019/881.

(2) Provedbena uredba (EU) 2024/482 temelji se na postojećim međunarodnim normama, odnosno na zajedničkim kriterijima i zajedničkoj evaluacijskoj metodologiji koje održavaju Međunarodna organizacija za normizaciju (ISO) i Međunarodna elektrotehnička komisija (IEC). U Provedbenoj uredbi (EU) 2024/482 upućuje se na norme ISO/IEC, ali se u njoj ne navodi koja se njihova verzija primjenjuje. Stoga bi trebalo utvrditi koja se verzija normi primjenjuje na certifikate izdane u okviru EUCC-a.

(3) Državne organizacije koje su pridonijele razvoju zajedničkih kriterija i zajedničke evaluacijske metodologije u okviru Sporazuma o priznavanju certifikata izdanih na temelju zajedničkih kriterija u području sigurnosti IT-a (CCRA) su, uz ISO/IEC, zajednički nositelji autorskih prava na njih. Te državne organizacije zadržavaju pravo na njihovo korištenje. Zbog njihove važnosti specifikacije koje izdaje CCRA trebale bi biti i osnova za certifikaciju u okviru EUCC-a.

(4) Kako bi se olakšala provedba zajedničkih kriterija i normi zajedničke evaluacijske metodologije, CCRA može davati njihova tumačenja, koja u obzir mogu uzimati centri za evaluaciju sigurnosti informacijske tehnologije (ITSEF) i certifikacijska tijela.

(5) Međunarodne norme koje se odnose na zajedničke kriterije mogu se ažurirati. Da bi prelazak bio uredan i na vrijeme, primjereno je definirati prijelazna pravila kako bi se dobavljačima, ITSEF-ovima i certifikacijskim tijelima te drugim relevantnim akterima dalo dovoljno vremena za potrebne prilagodbe. Ta prijelazna pravila trebalo bi u odgovarajućoj mjeri uskladiti s globalnim praksama, kao što su one koje je utvrdio CCRA.

([1]) SL L 151, 7.6.2019., str. 15., ELI: http://data.europa.eu/eli/reg/2019/881/oj.

([2]) Provedbena uredba Komisije (EU) 2024/482 od 31. siječnja 2024. o utvrđivanju pravila za primjenu Uredbe (EU) 2019/881 Europskog parlamenta i Vijeća u pogledu donošenja europskog programa kibernetičkosigurnosne certifikacije na temelju zajedničkih kriterija (EUCC) (SL L, 2024/482, 7.2.2024., ELI: http://data.europa.eu/eli/reg_impl/2024/482/oj).

(6) U Provedbenoj uredbi (EU) 2024/482 nije određeno dokad bi se certifikacija IKT proizvoda mogla temeljiti na prethodnim verzijama zajedničkih kriterija i normi zajedničke evaluacijske metodologije. Tehničke domene i profili zaštite iz priloga I., II. i III. toj provedbenoj uredbi temelje se na prethodnim verzijama normi ISO/IEC 15408 i 18045. U Provedbenoj uredbi (EU) 2024/482 stoga bi trebalo odrediti u kojim se okolnostima i dalje primjenjuje prethodna verzija zajedničkih kriterija i zajedničke evaluacijske metodologije te kako će se ostvariti prelazak na najnoviju verziju međunarodnih normi.

(7) U prijelaznom bi razdoblju relevantni dionici trebali dati prednost ažuriranju relevantnih tehničkih domena i profila zaštite. Provedbenom uredbom (EU) 2024/482 trebalo bi propisati da se potrebne sigurnosti koje se temelje na prethodnoj verziji normi prihvaćaju do 31. prosinca 2027. u skladu s prijelaznom politikom koju je donio CCRA. Međutim, treba napomenuti da ta prijelazna politika obuhvaća početne evaluacije proizvoda i profila zaštite koje su započete najkasnije 30. lipnja 2024., a na taj se datum EUCC još nije primjenjivao. Nadalje, u skladu s CCRA-ovom prijelaznom politikom Provedbenom uredbom (EU) 2024/482 trebalo bi propisati da se potrebne sigurnosti sukladne s tom provedbenom uredbom za koje je deklarirana sukladnost s profilima zaštite koji se temelje na prethodnoj verziji normi prihvaćaju do 31. prosinca 2027. Uz to, kad se na temelju Provedbene uredbe (EU) 2024/482 u kontekstu revizije nacionalnog certifikata izdaje novi certifikat koji počinje vrijediti unutar dvije godine od izdavanja izvornog certifikata, trebalo bi biti moguće koristiti prethodnu verziju normi. To se ne bi primjenjivalo u slučaju revizije kod koje nije potrebno izdavanje novog certifikata na temelju Provedbene uredbe (EU) 2024/482 i ako certifikat ostaje valjan.

(8) Radi urednog prelaska na najnoviju verziju normi Provedbenom uredbom (EU) 2024/482 trebalo bi utvrditi posebna prijelazna pravila i nastaviti omogućivati izdavanje, na temelju te provedbene uredbe, certifikata s deklariranom sukladnošću s profilima zaštite koji se temelje na prethodnim verzijama normi koje je objavio CCRA ako je korištenje takvih profila zaštite propisano zakonodavstvom Unije. To se odnosi na Provedbenu uredbu Komisije (EU) 2016/799 ([3]), Uredbu (EU) br. 910/2014 Europskog parlamenta i Vijeća ([4]) i Provedbenu odluku Komisije (EU) 2016/650 ([5]).

(9) U Prilogu I. Provedbenoj uredbi (EU) 2024/482 navode se primjenjive specifikacije najsuvremenijih tehnika za evaluaciju IKT proizvoda i profila zaštite. Međutim, ne navodi se verzija tih specifikacija. Stoga bi trebalo utvrditi koja se verzija tih specifikacija primjenjuje na certifikate izdane u okviru EUCC-a. Te se verzije temelje na specifikacijama koje je potvrdila Europska skupina za kibernetičkosigurnosnu certifikaciju (ECCG) te su dodatno preispitane kako bi se mogle uvrstiti u EUCC. Nadalje, Prilog I. trebalo bi izmijeniti kako bi se u njega uvrstile ažurirane i nove specifikacije najsuvremenijih tehnika koje je potvrdio ECCG, čime bi se postigla ujednačena akreditacija tijela za ocjenjivanje sukladnosti u okviru EUCC-a. Zahtjeve koji se odnose na akreditaciju ITSEF-ova trebalo bi ažurirati kako bi se pojasnila primjena kriterija neovisnosti i nepristranosti, a za akreditaciju certifikacijskih tijela trebalo bi odrediti novu specifikaciju najsuvremenijih tehnika.

(10) Specifikacije najsuvremenijih tehnika mogu se dodati u EUCC ili se mogu ažurirati u kontekstu aktivnosti njegova održavanja. Za nove ili ažurirane specifikacije najsuvremenijih tehnika možda će biti potrebno utvrditi odgovarajuća prijelazna pravila kako bi se dobavljačima, ITSEF-ovima, certifikacijskim tijelima i drugim dionicima omogućilo da provedu potrebne prilagodbe. Kad je riječ o ažuriranju specifikacije najsuvremenijih tehnika za akreditaciju ITSEF-ova, te bi se ažurirane specifikacije trebale primjenjivati na akreditacije izdane prije 8. srpnja 2025. samo kad se one revidiraju, primjerice u kontekstu postupka ocjenjivanja ili ponovnog ocjenjivanja. Uz to, ažurirane specifikacije trebale bi se primjenjivati na sve akreditacije ITSEF-ova izdane nakon 8. srpnja 2025.

([3]) Provedbena uredba Komisije (EU) 2016/799 od 18. ožujka 2016. o provedbi Uredbe (EU) br. 165/2014 Europskog parlamenta i Vijeća o utvrđivanju tehničkih zahtjeva za izradu, ispitivanje, ugradnju, rad i popravak tahografa i njihovih sastavnih dijelova (SL L 139, 26.5.2016., str. 1., ELI: http://data.europa.eu/eli/reg_impl/2016/799/oj).

([4]) Uredba (EU) br. 910/2014 Europskog parlamenta i Vijeća od 23. srpnja 2014. o elektroničkoj identifikaciji i uslugama povjerenja za elektroničke transakcije na unutarnjem tržištu i stavljanju izvan snage Direktive 1999/93/EZ (SL L 257, 28.8.2014., str. 73., ELI: http://data.europa.eu/eli/reg/2014/910/oj).

([5]) Provedbena odluka Komisije (EU) 2016/650 od 25. travnja 2016. o utvrđivanju normi za ocjenu sigurnosti kvalificiranih sredstava za izradu potpisa i pečata u skladu s člankom 30. stavkom 3. i člankom 39. stavkom 2. Uredbe (EU) br. 910/2014 Europskog parlamenta i Vijeća o elektroničkoj identifikaciji i uslugama povjerenja za elektroničke transakcije na unutarnjem tržištu (SL L 109, 26.4.2016., str. 40., ELI: http://data.europa.eu/eli/dec_impl/2016/650/oj).

(11) Dodatnim ispravcima članaka 5., 8., 16., 29. i 44. te Priloga IV. Provedbenoj uredbi (EU) 2024/482 ujednačuju se formulacije i postiže jasnije pravno tumačenje.

(12) Pravila za prijavljivanje tijela za ocjenjivanje sukladnosti trebala bi se utvrditi horizontalno za sve programe iz europskog okvira za kibernetičkosigurnosnu certifikaciju. Ta pravila za prijavljivanje obuhvaćena su Provedbenom uredbom Komisije (EU) 2024/3143 ([6]). Članke 23. i 24. Provedbene uredbe (EU) 2024/482 stoga bi trebalo izbrisati s danom početka primjene Provedbene uredbe (EU) 2024/3143.

(13) Provedbenu uredbu (EU) 2024/482 trebalo bi stoga na odgovarajući način izmijeniti i ispraviti.

(14) Mjere predviđene u ovoj Uredbi u skladu su s mišljenjem Odbora osnovanog člankom 66. Uredbe (EU) 2019/881,

DONIJELA JE OVU UREDBU:

Članak 1.

Provedbena uredba (EU) 2024/482 mijenja se kako slijedi:

(1) u članku 2. točke 1. i 2. zamjenjuju se sljedećim:

„1. ‚zajednički kriteriji' znači zajednički kriteriji za evaluaciju sigurnosti informacijske tehnologije kako su utvrđeni u normama ISO/IEC 15408-1:2022, ISO/IEC 15408-2:2022, ISO/IEC 15408-3:2022, ISO/IEC 15408-4:2022 ili ISO/IEC 15408-5:2022 ili u Zajedničkim kriterijima za evaluaciju sigurnosti informacijske tehnologije, verzija CC:2022, dijelovi od 1. do 5., koje su objavile stranke Sporazuma o priznavanju certifikata izdanih na temelju zajedničkih kriterija u području sigurnosti IT-a;

2. ‚zajednička evaluacijska metodologija' znači Zajednička metodologija za evaluaciju sigurnosti informacijske tehnologije kako je utvrđena u normi ISO/IEC 18045:2022, ili Zajednička metodologija za evaluaciju sigurnosti informacijske tehnologije, verzija CEM:2022, koju su objavile stranke Sporazuma o priznavanju certifikata izdanih na temelju zajedničkih kriterija u području sigurnosti IT-a;";

(2) članak 3. zamjenjuje se sljedećim:

„*Članak 3.*

Evaluacijske norme

1. Za evaluacije u okviru EUCC-a vrijede sljedeće norme:

(a) zajednički kriteriji;

(b) zajednička evaluacijska metodologija.

2. Do 31. prosinca 2027. certifikat se može izdati u okviru EUCC-a u kojem su primijenjene bilo koje od sljedećih normi:

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

(b) Zajednički kriteriji za evaluaciju sigurnosti informacijske tehnologije, verzija 3.1., revizija 5., koje su objavile stranke Sporazuma o priznavanju certifikata izdanih na temelju zajedničkih kriterija u području sigurnosti IT-a;

([6]) Provedbena uredba Komisije (EU) 2024/3143 od 18. prosinca 2024. o utvrđivanju okolnosti, formata i postupaka za prijave u skladu s člankom 61. stavkom 5. Uredbe (EU) 2019/881 Europskog parlamenta i Vijeća o ENISA-i (Agencija Europske unije za kibersigurnost) te o kibersigurnosnoj certifikaciji u području informacijske i komunikacijske tehnologije (SL L, 2024/3143, 19.12.2024., ELI: http://data.europa.eu/eli/reg_impl/2024/3143/oj).

(c) ISO/IEC 18045:2008;

(d) Zajednička metodologija za evaluaciju sigurnosti informacijske tehnologije, revizija 5., verzija 3.1., koju su objavile stranke Sporazuma o priznavanju certifikata izdanih na temelju zajedničkih kriterija u području sigurnosti IT-a.

3. Do 31. prosinca 2027. certifikat u kojem se primjenjuju norme iz stavka 1. može se izdati u okviru EUCC-a s deklariranom sukladnošću s profilom zaštite u kojem su primijenjene norme iz stavka 2.

4. Certifikat u kojem se primjenjuju norme iz stavka 1. također se može izdati u okviru EUCC-a s deklariranom sukladnošću s profilom zaštite u kojem je primijenjena jedna od sljedećih normi, pod uvjetom da je korištenje takvog profila zaštite propisano Provedbenom uredbom Komisije (EU) 2016/799 (*), Uredbom (EU) br. 910/2014 Europskog parlamenta i Vijeća (**) ili Provedbenom odlukom Komisije (EU) 2016/650 (***):

(a) Zajednički kriteriji za evaluaciju sigurnosti informacijske tehnologije, verzija 3.1, revizija od 1. do 4., koje su objavile stranke Sporazuma o priznavanju certifikata izdanih na temelju zajedničkih kriterija u području sigurnosti IT-a;

(b) Zajednička metodologija za evaluaciju sigurnosti informacijske tehnologije, verzija 3.1., revizija od 1. do 4., koju su objavile stranke Sporazuma o priznavanju certifikata izdanih na temelju zajedničkih kriterija u području sigurnosti IT-a;

_____

(*) Provedbena uredba Komisije (EU) 2016/799 od 18. ožujka 2016. o provedbi Uredbe (EU) br. 165/2014 Europskog parlamenta i Vijeća o utvrđivanju tehničkih zahtjeva za izradu, ispitivanje, ugradnju, rad i popravak tahografa i njihovih sastavnih dijelova (SL L 139, 26.5.2016., str. 1., ELI: http://data.europa.eu/eli/reg_impl/2016/799/oj).

(**) Uredba (EU) br. 910/2014 Europskog parlamenta i Vijeća od 23. srpnja 2014. o elektroničkoj identifikaciji i uslugama povjerenja za elektroničke transakcije na unutarnjem tržištu i stavljanju izvan snage Direktive 1999/93/EZ (SL L 257, 28.8.2014., str. 73., ELI: http://data.europa.eu/eli/reg/2014/910/oj).

(***) Provedbena odluka Komisije (EU) 2016/650 od 25. travnja 2016. o utvrđivanju normi za ocjenu sigurnosti kvalificiranih sredstava za izradu potpisa i pečata u skladu s člankom 30. stavkom 3. i člankom 39. stavkom 2. Uredbe (EU) br. 910/2014 Europskog parlamenta i Vijeća o elektroničkoj identifikaciji i uslugama povjerenja za elektroničke transakcije na unutarnjem tržištu (SL L 109, 26.4.2016., str. 40., ELI: http://data.europa.eu/eli/dec_impl/2016/650/oj).";

(3) u poglavlju IV. umeće se sljedeći članak 20.a:

„*Članak 20.a*

Specifikacija zahtjeva za akreditaciju tijela za ocjenjivanje sukladnosti

Pri akreditaciji tijela za ocjenjivanje sukladnosti uzima se u obzir specifikacija zahtjeva za akreditaciju certifikacijskih tijela i ITSEF-ova kako je utvrđeno u primjenjivim specifikacijama najsuvremenijih tehnika iz točke 2. Priloga I.";

(4) brišu se članci 23. i 24.;

(5) u članku 48. dodaje se sljedeći stavak 4.:

„4. Ako u Prilogu I. ili II. nije navedeno drukčije, specifikacije najsuvremenijih tehnika primjenjuju se od datuma početka primjene akta o izmjeni kojim su one uvrštene u Prilog I. ili II.";

(6) u članku 49. dodaje se sljedeći stavak 4.:

„4. Ako se revizija iz stavka 3. provodi unutar dvije godine od izdavanja početnog certifikata i ako se na temelju nje izda novi certifikat u skladu s ovom Uredbom, mogu se primijeniti norme iz članka 3. stavka 2. Datumom izdavanja početnog certifikata smatra se datum izdavanja posljednjeg certifikata za IKT proizvod ili profil zaštite na kojem se temelji postojeća certifikacija.";

(7) Prilog I. zamjenjuje se tekstom iz Priloga I. ovoj Uredbi;

(8) Prilog IV. mijenja se u skladu s Prilogom II. ovoj Uredbi.

Članak 2.

Provedbena uredba (EU) 2024/482 ispravlja se kako slijedi:

(1) u članku 5. stavku 1. točka (b) zamjenjuje se sljedećim:

„(b) uz deklariranje sukladnosti s certificiranim profilom zaštite kao dijelom IKT procesa ako IKT proizvod pripada kategoriji IKT proizvoda obuhvaćenoj tim profilom zaštite.”;

(2) članak 8. ispravlja se kako slijedi:

(a) naslov se zamjenjuje sljedećim:

„Informacije potrebne za certifikaciju i evaluaciju”;

(b) stavak 1. zamjenjuje se sljedećim:

„1. Podnositelj zahtjeva za certifikaciju na temelju EUCC-a certifikacijskom tijelu i ITSEF-u dostavlja ili na drugi način stavlja na raspolaganje sve informacije potrebne za certifikacijske i evaluacijske aktivnosti.”;

(3) članak 16. zamjenjuje se sljedećim:

„*Članak 16.*

Informacije potrebne za certifikaciju i evaluaciju profila zaštite

Podnositelj zahtjeva za certifikaciju profila zaštite certifikacijskom tijelu i ITSEF-u dostavlja ili na drugi način stavlja na raspolaganje, u potpunom i točnom obliku, sve informacije potrebne za certifikacijske i evaluacijske aktivnosti. Članak 8. stavci 2., 3., 4. i 7. primjenjuju se *mutatis mutandis*.”;

(4) u članku 17. briše se stavak 1.;

(5) u članku 29. stavak 2. zamjenjuje se sljedećim:

„2. Ako nositelj EUCC certifikata ne predloži odgovarajuće korektivne mjere u roku iz stavka 1., certifikat se suspendira u skladu s člankom 30. ili povlači u skladu s člankom 14. ili 20.”.

Članak 3.

Ova Uredba stupa na snagu dvadesetog dana od dana objave u *Službenom listu Europske unije*.

Članak 1. stavak 4. primjenjuje se od 8. siječnja 2025.

Ova je Uredba u cijelosti obvezujuća i izravno se primjenjuje u svim državama članicama.

Sastavljeno u Bruxellesu 18. prosinca 2024.

Za Komisiju
Predsjednica
Ursula VON DER LEYEN

PRILOG I.

„PRILOG I.

Specifikacije najsuvremenijih tehnika za tehničke domene i druge specifikacije najsuvremenijih tehnika

1. Specifikacije najsuvremenijih tehnika za tehničke domene na razini AVA_VAN 4 ili 5:
   (a) sljedeće specifikacije koje se odnose na usklađenu evaluaciju tehničke domene ‚pametne kartice i slični uređaji':
      (1) ‚Minimalni zahtjevi ITSEF-a za sigurnosne evaluacije pametnih kartica i sličnih uređaja', verzija 1.1;
      (2) ‚Minimalni sigurnosni zahtjevi za lokaciju', verzija 1.1;
      (3) ‚Primjena zajedničkih kriterija na integrirane krugove', verzija 1.1;
      (4) ‚Zahtjevi za sigurnosnu arhitekturu (ADV_ARC) za pametne kartice i slične uređaje', verzija 1.1;
      (5) ‚Certifikacija proizvoda s ‚otvorenom' tehnologijom pametnih kartica', verzija 1.1;
      (6) ‚Evaluacija složenih proizvoda za pametne kartice i slične uređaje', verzija 1.1;
      (7) ‚Primjena potencijala za napad na pametne kartice i slične uređaje', verzija 1.2;
   (b) sljedeće specifikacije koje se odnose na usklađenu evaluaciju tehničke domene ‚hardverski uređaji sa sigurnosnim kutijama':
      (1) ‚Minimalni zahtjevi za ITSEF za sigurnosne evaluacije hardverskih uređaja sa sigurnosnim kutijama', verzija 1.1;
      (2) ‚Minimalni sigurnosni zahtjevi za lokaciju', verzija 1.1;
      (3) ‚Primjena potencijala za napad na hardverske uređaje sa sigurnosnim kutijama', verzija 1.2.

2. Specifikacije najsuvremenijih tehnika koje se odnose na usklađenu akreditaciju tijela za ocjenjivanje sukladnosti:
   (a) ‚Akreditacija ITSEF-a za EUCC', verzija 1.1 za akreditacije izdane prije 8. srpnja 2025.;
   (b) ‚Akreditacija ITSEF-a za EUCC', verzija 1.6c za akreditacije koje su novoizdane ili revidirane nakon 8. srpnja 2025.;
   (c) ‚Akreditacija certifikacijskih tijela za EUCC', verzija 1.6.b.".

PRILOG II.

U Prilogu IV. Provedbenoj uredbi (EU) 2024/482, odjeljku IV.3., točke 5. i 6. zamjenjuju se sljedećim:

„5. Ako certifikacijsko tijelo potvrdi da je riječ o manjim promjenama, ne izdaje se novi certifikat za izmijenjeni IKT proizvod te se sastavlja izvješće o održavanju uz izvješće o početnoj certifikaciji.

Izvješće o održavanju uvrštava se kao dio izvješća o analizi utjecaja i sadržava sljedeće odjeljke:

(a) uvod;

(b) opis promjena;

(c) pojedinačni proizvođačevi dokazi koji su pod utjecajem.

6. Izvješće o održavanju iz točke 5. dostavlja se ENISA-i radi objave na njezinim internetskim stranicama o kibernetičko-sigurnosnoj certifikaciji.”.