REPUBLIKA E SHQIPËRISË
AUTORITETI KOMBËTAR PËR SIGURINË KIBERNETIKE

Nr. 2866 Prot. Tiranë më 03.11.2025

U R DH Ë R

Nr. 317 datë 03 / 11 / 2025

PËR MIRATIMIN E POLITIKËS PËR ZBULIMIN E KOORDINUAR TË VULNERABILITETEVE

Në zbatim të ligjit nr. 25/2024 "Për sigurinë kibernetike",

U R DH Ë R O J:

1. Miratimin e politikës "Për zbulimin e koordinuar të vulnerabiliteteve", sipas tekstit që i bashkëlidhet këtij urdhri dhe është pjesë përbërëse e tij.
2. Ngarkohen Autoriteti Kombëtar për Sigurinë Kibernetike, për zbatimin e këtij urdhri.
3. Ky urdhër hyn në fuqi menjëherë.

DREJTOR I PËRGJITHSHËM

IGLI T[illegible]

REPUBLIKA E SHQIPËRISË - AUTORITETI KOMBËTAR PËR SIGURINË KIBERNETIKE - I MINISTRAVE

Adresa: Rruga "Papa Gjon Pali II", Nr. 3, Kati 1, Tiranë;
Faqe web: www.aksk.gov.al E-mail: info@aksk.gov.al
Tel : 04 2221 039

POLITIKA E ZBULIMIT TË KOORDINUAR TË VULNERABILITETEVE (CVD)

1. Hyrje

Identifikimi dhe shfrytëzimi i vulnerabiliteteve shpesh përdoret për kompromentimin e informacionit dhe sigurisë së sistemeve dhe rrjeteve të informacionit të prekura. Këto vulnerabilitete mund të përdoren në kryerjen e krimeve kibernetike, krimeve ekonomike, vjedhjen e informacionit ose kredencialeve, si dhe në disa raste kanë rezultuar të lidhura edhe me sulme ndaj infrastrukturave strategjike në disa vende. Për këtë arsye është e rëndësishme të zbatohen politika për raportimin e trajtimin e vulnerabiliteteve.

Kjo politikë krijon një kornizë për raportimin dhe zbulimin e koordinuar të vulnerabiliteteve të identifikuara në produkte dhe shërbime TIK të prekura, duke siguruar pajtueshmërinë me ligjin nr. 25/2024 "Për sigurinë kibernetike" si dhe bazuar në praktikat më të mira ndërkombëtare.

Autoriteti Kombëtar për Sigurinë Kibernetike (AKSK), në cilësinë e koordinatorit për zbulimin e vulnerabiliteteve, është përgjegjës për zbatimin e kësaj politike me qëllim identifikimin dhe trajtimin e vulnerabiliteteve për të forcuar sigurinë kibernetike në nivel kombëtar.

Për zbatimin e kësaj politike, AKSK bashkëpunon me personat fizike dhe juridikë që raportojnë vulnerabilitete, të tillë si operatorët e infrastrukturave kritike dhe të rëndësishme të informacionit, kërkuesit e sigurisë, prodhuesit, shitësit, si dhe subjektet e tjera të interesuara, për të adresuar vulnerabilitetet e zbuluara dhe mbrojtur subjektet apo produktet ku ato zbulohen.

AKSK koordinon zbulimin dhe dokumentimin e vulnerabiliteteve në regjistrin e vulnerabiliteteve. Autoriteti, në zbatim të ligjit nr. 25/2024 "Për sigurinë kibernetike", identifikon, analizon dhe ofron asistencë për operatorët e infrastrukturave kritike dhe të rëndësishme të informacionit në rast të një vulnerabiliteti të identifikuar kryesisht apo të raportuar nga operatorët e infrastrukturave të informacionit. Gjithashtu, Autoriteti do të ndihmojë edhe për trajtimin e vulnerabiliteteve që zbulohen në subjekte të tjera, të raportuara nga persona fizikë apo juridikë.

2. Fusha e zbatimit

Kjo politikë zbatohet për vulnerabilitetet si më poshtë vijon:

- Vulnerabilitetet në aplikacione, software dhe sisteme;
- Vulnerabilitetet në pajisje, hardware dhe sisteme të integruara;

- Vulnerabilitetet në rrjetet dhe sistemet e informacionit, duke përfshirë infrastrukturat kritike dhe të rëndësishme të informacionit, si dhe institucionet qeveritare dhe të pavarura në Republikën e Shqipërisë.
- Vulnerabilitetet e raportuara nga persona të tjerë fizikë apo juridikë.

3. Përkufizimi i vulnerabilitetit dhe incidentet që lidhen me të

Çfarë është një vulnerabilitet?

Vulnerabiliteti është një dobësi, ndjeshmëri ose defekt i produkteve ose shërbimeve TIK, që mund të shfrytëzohet nga një kërcënim kibernetik. Një vulnerabilitet mund të çojë në një ngjarje që kompromenton sigurinë e një pajisjeje, sistemi operativ, aplikacioni, protokolli, rrjeti ose sistemi informacioni.

Nga dallohet një vulnerabilitet nga një incident i sigurisë kibernetike

Një vulnerabilitet është i ndryshëm nga një incident i sigurisë kibernetike, që është një ngjarje që ka një efekt real ose potencialisht negativ në sigurinë ose performancën e një sistemi. Incident i sigurisë kibernetike është çdo ngjarje që komprometon disponueshmërinë, vërtetësinë, integritetin, konfidencialitetin e të dhënave të ruajtura, të transmetuara apo të përpunuara ose të shërbimeve të ofruara apo të aksesueshme përmes rrjeteve dhe sistemeve të informacionit. Incidentet mund të vijnë si rezultat i shfrytëzimit të një vulnerabiliteti, por trajtohen veçmas dhe sipas procedurave përkatëse.

Shembuj të incidenteve të sigurisë kibernetike të lidhura me vulnerabilitetet përfshijnë si më poshtë vijon:

- **Tentativë ndërhyrjeje:**
  - Shfrytëzimi i vulnerabiliteteve të njohura: përpjekje për të kompromentuar një sistem ose për të ndërprerë një shërbim duke shfrytëzuar vulnerabilitetet (*buffer overflow, XSS, backdoor*, etj.).
  - Përpjekje të shumëfishta për akses me shkelje të kredencialeve (*brutte force*, thyerje fjalëkalimesh...).
  - Sulm i panjohur duke përdorur shfrytëzim.

- **Ndërhyrje:**
  - Kompromet im aplikacioni: kryhet duke shfrytëzuar vulnerabilitetet e software-t.

- **Mohim i disponueshmërisë:**
  - DoS/DdoS i referohet një incidenti kibernetike ku shumë pajisje të shpërndara në internet dërgojnë një sasi të madhe trafiku drejt një shërbimi, aplikacioni, faqeje web ose serveri, me qëllim që ta mbingarkojnë atë, për të ngadalësuar funksioninimin ose për të bërë të padisponueshëm shërvimin për përdoruesit duke e ndërprerë atë.

❖ **Shërbime dhe sisteme të cënueshme:**

- Shërbime të aksesueshme publikisht që mund të kenë kriptografi të dobët (serverat web të ndjeshëm ndaj sulmeve POODLE/FREAK, Heartbleed, FREAK...).
- Amplifikator DDoS: shërbime të aksesueshme publikisht që mund të përdoren për reflektim ose amplifikim të sulmeve DDoS, p.sh. duke shfrytëzuar funksionalitetin e serverit të hapur DNS që konverton emrat e domain-eve në adresa IP për të mbingarkuar një rrjet ose server specifik me një sasi të amplifikuar trafiku.
- Sistem i cenueshëm për arsye të ndryshme (konfigurim i dobët i proxy-t në një klient të Web Proxy Autodiscovery Protocol, sistem i vjetëruar, mungesë e antivirusit dhe/ose firewall-it...).

4. Kompetencat e Autoritetit në zbulimin e vulnerabiliteteve

Autoriteti Kombëtar për Sigurinë Kibernetike, në zbatim të nenit 9 dhe nenit 14 të ligjit nr. 25/2024 "Për sigurinë kibernetike", që vepron si CSIRT Kombëtar, në cilësinë e koordinatorit për zbulimin e vulnerabiliteteve kryen detyrat si më poshtë vijon:

a) identifikon dhe kontakton me subjektet e interesuara;

b) ndihmon personat fizikë ose juridikë që raportojnë një vulnerabilitet;

c) negocion afatet kohore të zbulimit dhe të menaxhimit të vulnerabiliteteve që prekin shumë subjekte.

CSIRT-i Kombëtar në cilësinë e koordinatorit për zbulimin e vulnerabiliteteve siguron marrjen e veprimeve korrekte nga operatorët e infrastrukturave të informacionit në lidhje me vulnerabilitetin e raportuar dhe siguron anonimitetin e operatorit që raporton këtë vulnerabilitet.

Kur një vulnerabilitet i raportuar prek infrastrukturat e informacionit të shteteve të tjera, CSIRT-i Kombëtar, kur është e nevojshme, bashkëpunon me CSIRT-të e shteteve të tjera të caktuara si koordinatorë mbi bazën e një marrëveshjeje të lidhur ndërmjet palëve.

CSIRT-i Kombëtar zhvillon dhe mirëmban një regjistër të vulnerabiliteteve të konstatuara, i cili përmban të dhënat si më poshtë:

a) informacionin që përshkruan vulnerabilitetin;

b) produktet TIK ose shërbimet TIK të prekura dhe nivelin e cenueshmërisë në lidhje me rrethanat në të cilat mund të shfrytëzohet;

c) udhëzime në lidhje me zgjidhjet e dhëna për zbutjen e rreziqeve, që vijnë nga vulnerabilitetet e zbuluara.

Gjithashtu, Autoriteti, në zbatim të nenit 30 të ligjit nr. 25/2024 "Për sigurinë kibernetike", është përgjegjës në lidhje me skanime të rrjeteve dhe sistemeve të operatorëve të infrastrukturave kritike dhe të rëndësishme të informacionit për efekt të kontrollit të masave të sigurisë në lidhje me vulnerabilitete të mundshme, në çdo rast, duke informuar paraprakisht operatorin e infrastrukturës së informacionit, duke siguruar transparencë të procesit dhe garantuar konfidencialitetin e informacionit.

Autoriteti ofron mbështetje për personat fizikë dhe juridikë që dëshirojnë të japin informacion duke raportuar një vulnerabilitet që kanë zbuluar dhe vepron duke anonimizuar të dhënat e raportuesit, përveç nëse raportuesi shprehet ndryshe në çdo kohë gjatë menaxhimit të vulnerabilitetit.

5. Veprime që nuk lejohen në kërkimin e vulnerabiliteteve

Gjatë procesit të kërkimit për të identifikuar vulnerabilitete të mundshme, është e domosdoshme të veprohet në përputhje me legjislacionin në fuqi. Raportimi i një vulnerabiliteti pranë Autoritetit nuk e përjashton raportuesin nga detyrimi për të vepruar në përputhje me legjislacionin në fuqi edhe në vijim pas raportimit të këtij vulnerabiliteti. Gjithashtu, kërkimi për gjetjen e vulnerabiliteteve nuk mund të përdoret si pretekst për të sulmuar një sistem ose ndonjë objektiv tjetër.

Veprimet që nuk lejohen përfshijnë si më poshtë vijon:
-përdorimi i inxhinierisë sociale;
-kompromentimi i një sistemi dhe ruajtja e aksesit në mënyrë të vazhdueshme;
-manipulimi i të dhënave të aksesuara me anë të shfrytëzimit të vulnerabiliteteve;
-përdorimi i programeve keqdashëse;
-përdorimi i vulnerabiliteteve për çdo qëllim përtej vërtetimit të ekzistencës së tyre. Për të treguar ekzistencën e vulnerabilitetit, mund të përdoren metoda jo-agresive, për shembull duke renditur një drejtori sistemi;
-përdorimi i *brutte force* për të fituar akses në sisteme;
-ndarja e vulnerabiliteteve me palë të treta;
-kryerja e sulmeve DoS ose DDoS.

Të gjitha aktivitetet kërkimore për identifikimin e vulnerabiliteteve duhet të jenë në përputhje me legjislacionin në fuqi dhe rregullat e përcaktuara në këtë politikë.

Të gjitha vulnerabilitetet duhet të raportohen menjëherë pranë Autoritetit Kombëtar për Sigurinë Kibernetike sapo zbulohen dhe të mos shfrytëzohen në asnjë mënyrë.

Ndalohet që vulnerabiliteti i identifikuar dhe i raportuar pranë Autoritetit të bëhet i njohur për publikun nga raportuesi apo persona të tjerë, përpara se ky vulnerabilitet të trajtohet nga subjektet përgjegjëse dhe përpara se Autoritetit të marrë vendimin që publikimi i vulnerabilitetit nuk përbën më rrezik për shfrytëzimin e mundshëm të tij për qëllime keqdashëse.

6. Raportimi i një vulnerabilitetit

Vulnerabilitetet raportohen në AKSK nëpërmjet kanaleve të komunikimit si më poshtë:

- postës elektronike, email: info@aksk.gov.al;
- telefonit: 04 2221 039.

Operatorët e infrastrukturave kritike dhe të rëndësishme të informacionit mund të raportojnë për vulnaribilitetet e identifikuara edhe përmes Sistemit të Menaxhimit të Raportimit të Incidenteve, nëse ka pasur tentativa për ta shfrytëzuar vulnerabilitetin.

Rekomandohet që informacioni në përmbajtje të raportimit të enkriptohet me çelësin publik që lidhet me këtë email. Çelësin publik për përdorim mund ta shkarkoni këtu: https://aksk.gov.al/link-celes-publik/ .

Raportimet mund të kenë të bëjnë me vulnerabilitete në aplikacione dhe softuer, pajisje, harduer ose sisteme të integruara, si dhe sisteme dhe rrjete informacioni, duke përfshirë sistemet qeveritare dhe infrastrukturat kritike dhe të rëndësishme të informacionit.

6.1 Informacioni i kërkuar për raportim

Për të raportuar një vulnerabilitetet nevojitet informacioni si më poshtë vijon:
• përshkrim i qartë dhe i detajuar i vulnerabilitetit;
• informacion i qartë dhe i detajuar se si u zbulua vulnerabiliteti.
Informacione të tjera që mund të jenë të dobishme gjatë raportimit të vulnerabilitetit përfshijnë si më poshtë vijon:
• prova të qarta të ekzistencës së vulnerabilitetit nëpërmjet pamjeve të ekranit, linqeve, etj.);
• kur u zbulua vulnerabiliteti;
• çdo informacion që konsiderohet i nevojshëm për të lokalizuar dhe zgjidhur vulnerabilitetitn sa më shpejt dhe me efikasitet.

Me marrjen e raportimit dhe informacionit përkatës, AKSK do të konfirmojë marrjen e tij dhe mund të kërkojë sqarime dhe informacione të mëtejshme nëse është e nevojshme me qëllim trajtimin e vulnerabilitetit. AKSK do të fillojë komunikimin me palët e interesuara menjëherë për trajtimin e vulnerabilitetit. Nëse vulnerabiliteti përfshin një operator të infrastrukturës kritike apo të rëndësishme të informacionit, ekipet teknike të specializuara të Autoritetit ofrojnë mbështetje për të zbutur ndikimin dhe korrigjuar vulnerabilitetin sa më shpejt të jetë e mundur.

6.2 Vlerësimi dhe zgjidhja e vulnerabilitetit

Kur AKSK merr një raportim për një vulnerabilitet, hapi i parë është verifikimi nëse vulnerabilitet i raportuar është një vulnerabilitetet i ri në një sistem, rrjet informacioni apo produkt, apo është një incident i përdoruesit fundor.

Në rast të konstatimit se kemi të bëjmë me një vulnerabilitet të ri, ekipi i Autoritetit e menaxhon atë duke koordinuar komunikimin midis raportuesit dhe zotëruesit të produktit, sistemit apo

rrjetit të prekur. Pas zgjidhjes së vulnerabilitetit, Autoritetit e dokumenton atë si një vulnerabilitet të ri në regjistrin e vulnerabiliteteve, si dhe koordinon zbulimin publik të vulnerabilitetit duke anonimizuar informacionin sensitiv.

Në rastin e një incidenti të përdoruesit fundor, ekipi i menaxhimit të incidenteve të Autoritetit do të bëjë vlerësimin dhe prioritizimin (*triage*) si dhe klasifikimin e incidentit, duke njoftuar përdoruesit e prekur dhe subjektet e interesuara dhe duke ndarë detajet dhe zgjidhjet teknike, duke respektuar anonimatin e raportuesit.

6.3 Zbulimi i vulnerabilitetit për publikun

Zbulimi i vulnerabilitetit për publikun ndodh vetëm pas zbutjes së ndikimit dhe zgjidhjes së vulnerabilitetit, në koordinim me raportuesin dhe palët e prekura, dhe vetëm pasi Autoriteti vendos që publikimi i vulnerabilitetit nuk përbën më rrezik për shfrytëzimin e mundshëm të tij për qëllime keqdashëse. Zbulimi i vulnerabilitetit duke anonimizuar informacionin sensitiv bëhet në faqen zyrtare dhe në rrjetet sociale të Autoritetit dhe regjistrohet në regjistrin e vulnerabiliteteve.

7. Gatishmëria, Mbështetja dhe Komunikimi

CSIRT Kombëtar është në gatishmëri për përgjigjen dhe reagimin ndaj incidenteve dhe vulnerabiliteteve 24/7, duke ofruar mbështetje për trajtimin dhe zgjidhjen në kohë të vulnerabiliteteve që raportohen.

Për vulnerabilitetet që lidhen me operatorët e infrastrukturës kritike dhe të rëndësishme të informacionit, komunikimi me AKSK për raportimin dhe zgjidhjen e vulnerabiliteteve realizohet përmes pikave të kontaktit të dedikuara për të siguruar komunikim të shpejtë dhe mbështetje për zbutjen e ndikimit, trajtimin dhe zgjidhjen e tyre.