

BULETIN JAVOR

18-22 SHTATOR 2023



Shprehja

"Ajo që hakerët bëjnë është të hulumtojnë teknologjinë dhe të eksperimentojnë me të në mënyra që shumë njerëz nuk e imagjinojnë kurrë."

Emmanuel Goldstein

e javës

Përmbajtja:

- AKCESK pjesmarrës në panairin "Future2Tech"
- Autoriteti Kombëtar për Cesk në Konferencën BSidesTirana
- Gjigandi i teknologjisë Microsoft – partner strategjik i AKCESK



AKCESK pjesmarrës në panairin "Future2Tech"

Në panairin e inovacionit Future2Tech, Drejtori i Përgjithshëm i AKCESK Z. Igli Tafa prezantoi progresin e Autoritetit, si një partner të besueshëm të infrastrukturave kritike të informacionit, mbi menaxhimin e rrezikut kibernetik dhe rritjen e sigurisë në nivel kombëtar ndaj sulmeve kibernetike të sofistikuara.

Partneriteti i brendshëm dhe i jashtëm përfaqëson një nga shtyllat e vizionit të sigurisë kibernetike të Autoritetit.

Siguria kibernetike është përgjegjësi e përbashkët. E ardhmja do të jetë edhe më e sigurt nëse bashkërendojmë përpjekjet tona dhe mendojmë globalisht, në terma të adresimit të sfidave të sigurisë në ekosistemin digjital.



Autoriteti Kombëtar për Cesk në Konferencën BSidesTirana

Në konferencën BSides Tirana, Drejtori i Përgjithshëm i AKCESK Z. Igli Tafa, adresoi prioritetet e Autoritetit drejt një ekosistemi kibernetik të sigurt, në terma të investimeve teknologjike, rritjes së kapaciteteve njerëzore dhe rritjes së bashkëpunimit me infrastrukturat kritike të sektorit privat.

Maksimalisht të përkushtuar për të përballuar me sukses sfidat e së ardhmes dhe për të jetësuar vizionin strategjik të Autoritetit.



Gjigandi i teknologjisë Microsoft – partner strategjik i AKCESK

Autoriteti Kombëtar për Certifikimin Elektronik dhe Sigurinë Kibernetike dhe gjigandi i teknologjisë Microsoft, organizuan sot një takim të përbashkët me infrastrukturat kritike të informacionit, për rritjen e bashkëpunimit për një ekosistem digjital të sigurt në Shqipëri.

Partneriteti me këtë lider teknologjike, mbështetet në dy shtylla kryesore: implementimi i zgjidhjeve teknologjike të sigurta në treg dhe ngritja e kapaciteteve profesionale.

Microsoft, si një kompani lider në fushën e teknologjisë së informacionit dhe sigurisë kibernetike, ofroi hapësira bashkëpunimi për Autoritetin, duke treguar edhe një herë gadishmërinë e tij për të mbështetur Shqipërinë në rrugën e transformimit digjital dhe revolucionit kibernetik.



BULETINI JAVOR

18-22 SHTATOR 2023



Shprehja

"Ajo që hakerët bëjnë është të hulumtojnë teknologjinë dhe të eksperimentojnë me të në mënyra që shumë njerëz nuk e imagjinojnë kurrë."

Emmanuel Goldstain

e javës

Përmbajtja:

- FBI dhe CISA paralajmërojnë për sulme Ransomware
- Një problem në aplikacionin T-Mobile i lejoj përdoruesit të shihnin informacione nga llogaritë e njerëzve të tjerë
- Sulmuesit kibernetik APT36 infektjnë pajisjet Android duke përdorur klonet e aplikacionit YouTube
- GitLab - patching alert



FBI dhe CISA paralajmërojnë për sulme Ransomware

FBI dhe CISA paralajmëruan së fundmi infrastrukturën kritike për sulme të mundshme nga grupi i krimit kibernetik Snatch. Përpara se të vendosin ransomware, sulmuesit Snatch qëndrojnë deri në tre muaj në rrjetet e viktimave, duke kërkuar të dhëna të vlefshme për të eksfiltruar dhe për të identifikuar sistemet që mund të kodojnë.

FBI dhe CISA kanë publikuar një sërë masash zbutëse të rekomanduara që organizatat mund të zbatojnë për të përmirësuar masat e tyre të sigurisë kibernetike.

[Link:Lexo më shumë](#)



Sulmuesit kibernetik APT36 infektjnë pajisjet Android duke përdorur klonet e aplikacionit YouTube

Grupi i njohur kibernetik APT36, është duke shpërndarë së fundmi trojanin CapraRAT Remote Access (RAT) përmes tre aplikacioneve keqdashëse Android që imitojnë YouTube.

Pasi malware është instaluar në pajisjen e viktimës, ai mund të mbledhë të dhëna, të regjistrojë audio dhe video ose të ketë akses në informacione të ndjeshme komunikimi, në thelb duke funksionuar si një mjet spyware.

Kjo fushatë u zbulua nga studuesit e SentinelLabs, të cilët paralajmërojnë njerëzit dhe organizatat që të jenë shumë të kujdesshëm ndaj aplikacioneve të YouTube Android të hostuara në sajte të palëve të treta.

[Link:Lexo më shumë](#)



Një problem në aplikacionin T-Mobile i lejoj përdoruesit të shihnin informacione nga llogaritë e njerëzve të tjerë

Një defekt në aplikacionin T-Mobile lejoj disa klientë pasi logoheshin, të shihnin llogarinë dhe informacionin e faturimit të shumë njerëzve.

Informacioni i ekspozuar përfshinte emrat e klientëve, numrat e telefonit, adresat, gjendjet e llogarisë dhe detajet e kartës së kreditit.

Sipas një deklaratë nga kompania, ky ishte një gabim i përkohshëm i sistemit të cilën e zgjidhën shumë shpejt.

[Link:Lexo më shumë](#)

PATCHING ALERT



GitLab publikon përditësime sigurie emergjente

GitLab ka publikuar përditësime sigurie për të adresuar një vulnerabilitet kritik që prek versionet e GitLab Enterprise Edition (EE) nga 13.12 deri në 16.2.7, si dhe nga 16.3 deri në 16.3.4.

Dobësia identifikohet si CVE-2023-5009 dhe shfrytëzimi i tij mund të lejojë një sulmues të aksesojë informacione të ndjeshme.

Vulnerabiliteti u rregullua në versionet 16.3.4 dhe 16.2.7 të GitLab.

[Link:Lexo më shumë](#)