BULETIN JAVOR
26-30 QERSHOR
2023

Shprehja e javës

"Asnjë teknologji që është e lidhur me internetin nuk është e pahakueshme." - Abhijit Naskar

AKCESK pjesmarrëse në aktivitetin Cyber Week në Tel Aviv

Në kuadër të marrëveshjes së bashkëpunimit me Izraelin, AKCESK morri pjesë aktivisht në aktivitetin "Cyber week", i cili është një ngjarje e madhe vjetore ndërkombëtare e sigurisë kibernetike, e organizuar çdo vit në Universitetin e Tel Avivit. Gjatë tetë viteve të fundit, Java Kibernetike është vlerësuar ndërkombëtarisht si një nga ngjarjet kryesore të sigurisë kibernetike në botë.

Në një nga panelet e këtij aktiviteti u prezantua Platforma Crystal Ball, një platformë që përfshin vende dhe partneritete e cila mundëson analizën dhe ndarjen e informacionit në një mënyrë interaktive, të shpejtë, të sigurt dhe të lehtë midis vendeve për çështjet e mbrojtjes kibernetike. Ajo cfarë u evidentua si në aspektin e teknologjise dhe të ndërveprimit në fushën e sigurisë kibernetike ishte se sfidat e përbashkëta të sigurise kibernetikë, tejkalohen duke punuar së bashku, duke ndarë njohuritë, eksperiencat dhe teknologjitë për mbrojtje më të mirë dhe më të shpejt.

Gjatë kësaj jave, Zëvendës drejtori i përgjithshëm i AKCESK, zhvilloi një sërë takimesh me përfaqësues të institucioneve homologe nga vendet e tjera pjesëmarrëse, si dhe me industrinë, në terma të rritjes së bashkëpunimit mes vëndeve dhe implementimit të zgjidhjeve teknologjike të reja .

Dialogu Rregullator midis Bashkimit Europian dhe Ballkanit Perëndimor në Konferencën Sigurisë Kiberentike në Bruksel

Në datën 30 Qershor 2023 u organizua në Bruksel, takimi i dytë me Komisionin Europian mbi "Dialogun Rregullator midis Bashkimit Europian dhe Ballkanit Perëndimor". Gjithashtu në datat 28-29 Qershor 2023 u zhvillua workshop "Bashkëpunimi Rajonal në Rast të Incidenteve Potenciale Kibernetike" në kuadër të procesit të Berlinit, për të forcuar kapacitetet e sigurisë kibernetike në rajonin e Ballkanit Perëndimor.

Gjatë pjesëmarrjes së saj, AKCESK mori pjesë në 2 panele:

1.How Regional Cooperation Strengthens Cybersecurity – Opportunity and Approaches
2.EU Cyber Ecosystem : Lessons Learned and Opportunities for the Westernbalkans.
Në të dy panelet u diskutuan çështje mbi rëndësinë e bashkëpunimit rajonal dhe ndërkombëtar si dhe cilat ishin mësimet e marra mbi problematikat e hasura, praktikat më të mira dhe planet për ngritjen e niveleve të sigurisë kibernetike në nivel rajonal.

Takimi me Komisionin Europian

Gjatë takimit me përfaqësuses të Komisionit Europian, nga ana e përfaqësuesve të KE u trajtuan tema si:

- Open Data Directive - Non localization, free flow of non personal data
- Data Governance Act
- Cybersolidarity Act
- EU Cybershield

Nga ana e AKCESK u be një prezantim i punës së bërë nga Autoriteti mbi:

- Përafrimin e kuadrit ligjor mbi sigurinë kibernetike në përputhje me kërkesat e direktivave evropiane NIS1 dhe NIS2,
- Përmirësimin e kuadrit ligjor mbi shërbimet e besuara me eIDAS,
- Mbështetja mbi metodologjitë, rregulloret dhe direktivat e ENISA,
- Ndryshimet në planet strategjike në çështjet e qeverisjes kibernetike,
- Rritja e kapaciteteve teknike mbi sigurinë kibernetike
- Rritja e bashkëpunimit rajonal dhe ndërkombëtar
- Rritja e bashkëpunimit me kompanitë private.

Në fund të fjalës u kërkua nga AKCESK edhe rritja e bashkëpunimit dhe asistencës së Komisionit Evropian mbi përmirësimin e kuadrit ligjor dhe procedural në përputhje të plotë me kërkesat dhe standardet e BE.

Rruga "Papa Gjon Pali II", No.3 info@cesk.gov.al
Autoriteti Kombëtar për CESK
autoriteti_kombetar_cesk
+35542221039

BULETIN JAVOR
26-30 QERSHOR
2023

Sfrehja e javës

"Asnjë teknologji që është e lidhur me internetin nuk është e pahakueshme." - Abhijit Naskar

Përmbajtja:

- **Një vulnerabilitet kritik i sigurisë në WordPress plugin ekspozon llogaritë e përdoruesve**
- **Kompania Jumsec identifikon dërgimin e një malware në Microsoft Teams**
- **MOVEit Data breach**
- **Goole Chrome 114- Patching Alert**

Një vulnerabilitet kritik i sigurisë në WordPress plugin ekspozon llogaritë e përdoruesve

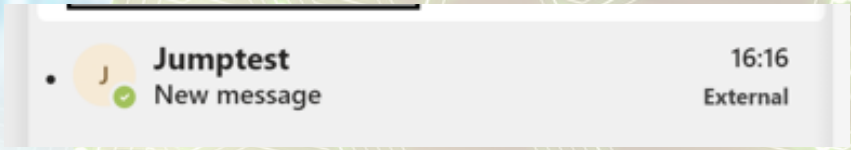
Rreth 200,000 faqe interneti të WordPress janë në rrezik të sulmeve të vazhdueshme duke shfrytëzuar një dobësi kritike të sigurisë .

Vulnerabiliteti i identifikuar si **CVE-2023-3460** mund të shfrytëzohet nga sulmues të paautentikuar për të krijuar llogari të reja përdoruesish me privilegje administrative, duke u dhënë atyre fuqinë për të marrë kontrollin e plotë të faqeve të prekura.

Çështja doli në dritë pasi u shfaqën raporte për shtimin e llogarive mashtruese të administratorëve në faqet e prekura, duke nxitur mirëmbajtësit të lançojnë rregullime të pjesshme në versionet 2.6.4, 2.6.5 dhe 2.6.6. Një përditësim i ri pritet të dalë në ditët në vijim.

Rekomandohet gjithashtu që të auditohen të gjithë përdoruesit e nivelit të administratorit në faqet e internetit për të përcaktuar nëse janë shtuar llogari të paautorizuara.

Link:Lexo më shumë



Kompania Jumsec identifikon dërgimin e një malware në Microsoft Teams

Hulumtues nga kompania e shërbimeve të sigurisë Jumpsec kanë identifikuar një metodë për të dërguar malware nëpërmjet Microsoft Teams.

Metodologjia e sulmit mbështetët në anashkalimin e kufizimeve të aplikacionit mbi dokumentet me burim të jashtëm.

Kjo ure komunikimi, përveçse mund të përdoret ne vetvete në aktet e Social Engineering dhe phishing, mundëson edhe dërgimin e një payloadi keqdashës në adresë të objektivit.

Këshillohen kompanitë dhe Institucionet që përdorin Microsoft Teams dhe nuk komunikojnë në mënyrë të rregullt me përdorues të jashtëm të çaktivizojnë këtë opsion në Microsoft Teams Admin Center.

Link:Lexo më shumë

Sulmet kibernetike ekspozojnë të dhëna të ndjeshme për studentët dhe stafin e shkollave publike

Një sulm kibernetik ka ekspozuar të dhëna të ndjeshme për rreth 45 mijë studentë të Shkollës Publike të Nju Jorkut - si dhe stafin e Departamentit të Arsimit dhe ofruesit e shërbimeve.

Dokumentet që janë aksesuar përfshijnë vlerësimet e studentëve dhe të dhënat e ekspozuara përfshijnë numrat e sigurimeve shoqërore dhe datat e lindjes.

Sulmuesit kibernetikë filluan të synonin një dobësi të panjohur më parë në softuerin popullor të transferimit të skedarëve ***MOVEit*** duke bërë të mundur infektimin e 150 organizatave, të cilat kompromet uan të dhënat personale të mbi 16 milionë individëve.

Deri më tani asnjë nga të dhënat e vjedhura nga studentët e shkollave publike nuk është publikuar .

Link: Lexo më shumë

PATCHING ALERT

Chrome 114 përditëson një vulnerabilitet kritik

Google së fundmi njoftoi një përditësim të ri të Chrome 114 që rregullon gjithsej katër vulnerabilitete duke përfshirë tre gabime kritike të raportuara nga studiues të jashtëm.

Vulnerabilitetet kritike, të cilat shkaktojnë dëmtim të kujtesës me të cilin Google ka qenë duke luftuar si në Chrome ashtu edhe në Android, mund të çojnë në ekzekutim arbitrar të kodit, korrupsion të të dhënave ose mohim të shërbimit.

Përditësimet fundit të Chrome shfaqen si versioni 114.0.5735.198 për macOS dhe Linux dhe si versionet 114.0.5735.198/199 për Windows.

AKCESK rekomandon te gjithë përdoruesit e Google Chrome të kryjnë përditësimet e nevojshme

Link: Lexo më shumë

Rruga "Papa Gjon Pali II", No.3 info@cesk.gov.al
Autoriteti Kombëtar për CESK
autoriteti_kombetar_cesk
+35542221039