BULETIN JAVOR
25-29 SHTATOR 2023

Shprehja e javës

"Mungesa e sigurisë në fazat fillestare të Inxhinierisë së Sistemeve është hendeku dhe rreziku më i madh i sigurisë kibernetike, në zhvillimin e sistemit modern."

Linda Rawson

Përmbajtja:

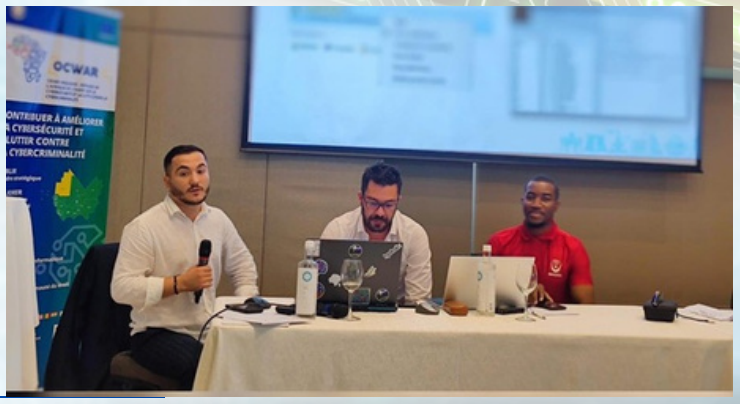
- **AKCESK pjesëmarrës në trajnimin për bashkëpunimin ndërinstitucional rajonal CSIRT/LEA**
- **AKCESK - Anëtari i 114 i Forumit Global të Ekspertizës Kibernetike (GFCE)**

AKCESK pjesëmarrës në trajnimin për bashkëpunimin ndërinstitucional rajonal CSIRT/LEA

Në vijim të aktiviteteve për rritjen e kapaciteteve njerëzore në fushën e sigurisë kibernetike, Autoriteti Kombëtar për Cesk, mori pjesë në trajnimin për bashkëpunimin ndërinstitucional CSIRT/LEA Rajonale, të organizuar në Port Luis, Mauritius, në datat 25-29 Shtator 2023, në kuadër të projekteve të bashkëfinancuara nga Bashkimi Evropian dhe Këshilli i Evropës, GLACY+ dhe OCWAR-C.

Synimi i trajnimit ishte fuqizimi i bashkëpunimit CERT-LEA, me fokus shkëmbimin e informacionit dhe përthithjen e njohurive praktike në terma teknike si Digital Forensics, Electronic evidences, OSINT investigation, malware analysis, bitcoin seizure, etj.

Pjesëmarrja e përfaqësuesve të AKCESK u vlerësua dhe u veçua në grup, për kontributin dhe prezantimin dinjitoz të zgjidhjeve të skenarëve, gjatë Table Top Exercise.



AKCESK - Anëtari i 114 i Forumit Global të Ekspertizës Kibernetike (GFCE)

Në kuadër të arritjes së objektivave strategjikë, në terma të fuqizimit të kapaciteteve njerëzore në fushën e sigurisë kibernetike, Autoriteti Kombëtar për Certifikimin Elektronik dhe Sigurinë Kibernetike ka finalizuar me sukses procesin e anëtarësimit në Forumin Global të Ekspertizës Kibernetike.

AKCESK, në cilësinë e anëtarit të GFCE, do të kontribuojë në mënyrë efektive, në adresimin e nevojave kombëtare, në rritjen e bashkëpunimit dhe koordinimin efektiv ndërkombëtar për ndërtimin e kapaciteteve, me qëllim rritjen e nivelit të sigurisë kibernetike në nivel rajonal dhe global.

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

BULETINI JAVOR
25-29 SHTATOR 2023

Shprehja e javës

"Mungesa e sigurisë në fazat fillestare të Inxhinierisë së Sistemeve është hendeku dhe rreziku më i madh i sigurisë kibernetike, në zhvillimin e sistemit modern."

Linda Rawson

Përmbajtja:

Cisco paralajmëron për vulnerabilitete në software-in IOS dhe IOS XE pas përpjekjeve për shfrytëzim

Cisco është duke paralajmëruar për tentativa shfrytëzimi të një vulnerabiliteti sigurie në software-in e saj IOS dhe IOS XE, i cili lejon ekzekutimin e kodit në distancë në sistemet e prekura.

Vulnerabiliteti identifikohet si CVE-2023-20109 dhe ka CVSS prej 6.6. Ai ndikon në të gjitha versionet e software-it që kanë të aktivizuar protokollin GDOI ose G-IKEv2.

Link:Lexo më shumë

Një malware i identifikuar si ZenRat shenjëstron përdoruesit e Windows

Sipas studiuesve të Proofpoint, një lloj i ri malware i quajtur ZenRAT është zhvilluar për të vjedhur informacione nga sistemet Windows dhe shpërndahet përmes instalimit të paketave të rreme për menaxhimin e fjalëkalimeve.
ZenRAT, pasi instalohet, mbledh informacione të rëndësishme si: emri i CPU-së, emri i GPU-së, versioni i sistemit të operimit, RAM-i ose adresa e IP-së dhe aplikacionet e instaluara.

Për të zbutur kërcënime të tilla, rekomandohet që përdoruesit të shkarkojnë *software* vetëm nga burime të besueshme dhe të sigurojnë vërtetësinë e faqeve të internetit.

Link: Lexo më shumë

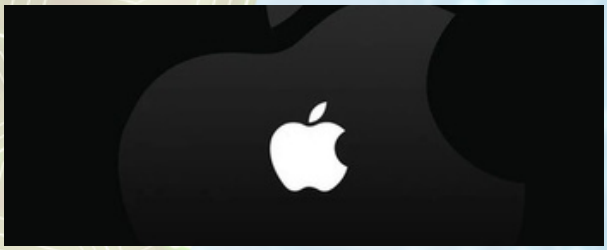
Sulmi masiv i MOVEit numëron më shumë se 2000 viktima

Gjatë muajit Maj grupi i sulmuesve kibernetik Cl0p nisi një fushatë sulmi masiv duke shfrytëzuar një vulnerabilitet të tipit zero-day në softuerin MOVEit për të vjedhur të dhënat e ruajtura në serverët e transferimit të skedarëve .

Coveware, një organizatë e reagimit ndaj incidenteve të sulmeve ransomware, vlerëson se sulmuesit Cl0p mund të kenë fituar nga 75 milion deri në 100 milion dollarë nga pagesat e shpërblimit vetëm në ditët e para të fushatës së sulmit masiv.

Link: Lexo më shumë

PATCHING ALERT



Apple - patching alert

Apple ka publikuar përditësime urgjente të sigurisë për të rregulluar tre vulnerabilitete të reja të shfrytëzuara në sulmet që synojnë përdoruesit e iPhone dhe Mac, të identifikuar si CVE-2023-41991 , CVE-2023-41993 dhe CVE -2023-41992 .

Tre vulnerabilitetet e reja janë korigjuar në versionet macOS 12.7/13.6, iOS 16.7/17.0. 1, iPadOS 16.7/17.0.1, watchOS 9.6.3/10.0.1 dhe versioni Safari 16.6.1.

AKCESK rekomandon të gjithë përdoruesit e produkteve të Apple të kryejnë përditësimet e fundit.
Link: Lexo më shumë

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