BULETIN JAVOR
15-19 MAJ 2023

Sharenja e javës

"Siguria kibernetike është shumë më tepër se një çështje IT"

Përmbajtja:

Përditësim i rëndësishëm sigurie për Wordpress

Një vulnerabilitet i zbuluar së fundmi në platformën Wordpress, i identifikuar si CVE-2023-30777, po shfrytëzohet në mënyrë aktive nga sulmuesit.

Vulnerabiliteti i tipit XSS (Cross-site scripting) lejon aksesimin e informacioneve të ndjeshme dhe eskalimin e privilegjeve në faqet e infektuara të ndërtuara me WordPress.

Administratorët e faqeve të WordPress këshillohen të aplikojnë menjëherë përditësimet e "Advanced Custom Fields" në versionet 5.12.6 dhe 6.1.6, për t'u mbrojtur nga aktivitetet e skanimit dhe shfrytëzimit të dobësive.

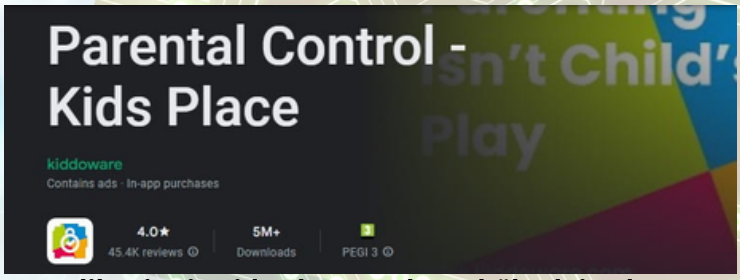
Link: Lexo më shumë

Sulm ndaj të dhënave personale në Departamentin Amerikan të Transportit

Departamenti Amerikan i Transportit (USDoT) raportoi se janë ekspozuar në një sulm kibernetik të dhënat personale të 237,000 punonjësve të mëparshëm dhe aktualë. Sulmi nuk ka sjellë pasoja në asnjë sistem tjetër dhe është izoluar në kohë nga sistemet e funksioneve administrative.

Agjencitë federale dhe punonjësit e tyre kanë qenë target i sulmeve kibernetike edhe më parë.

Link: Lexo më shumë



Aplikacioni "Kids Place" vulnerabël ndaj sulmeve

Studiuesit kanë zbuluar pesë vulnerabilitete në aplikacionin "Kiddoware Kids Place Parental Control" për Android.

Dobësitë i lejojnë sulmuesit të ngarkojnë skedarë infektues në pajisjet e fëmijëve, të vjedhin kredencialet e përdoruesve dhe t'i lejojnë fëmijët të anashkalojnë kufizimet e vendosura në aplikacion pa e vënë re prindërit.

Përdoruesit këshillohen të përditësojnë menjëherë versionin më të fundit 3.8.50 në Google Play për të mbrojtur sigurinë dhe privatësinë.

Link: Lexo më shumë

PATCHING ALERT

Përditësime sigurie nga Apple

Apple ka publikuar përditësime sigurie për 3 vulnerabilitete WebKit Zero-Day, të cilat mund të prekin iPhone dhe Mac.

Vulnerabilitet, të cilat mund të çojnë në ekspozim të informacioneve personale, janë korigjuar në sistemet e operimit iOS 16.5 and iPadOS 16.5.

AKCESK rekomandon të gjithë përdoruesit e Apple të instalojnë përditësimet.

Link: Lexo më shumë

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

BULETIN JAVOR
15-19 MAJ 2023

Përmbajtja:

- **Mbrojtja nga sulmet kibernetike dhe rritja e sigurisë për sistemet Industriale**
- **Ngritja e kapaciteteve në fokus të "Balkan CyberSecurity Days"**
- **Phishing Alert për sektorin e turizmit**

Mbrojtja nga sulmet kibernetike dhe rritja e sigurisë për sistemet Industriale

Në kuadër të ngritjes së kapaciteteve teknike të Infrastrukturave Kritike, të cilat funksonojnë mbi Sistemet Industriale, AKCESK mori pjesë në trajnimin ICS 301L të zhvilluar nga "CyberSecurity and Infrastucture Security Agency (CISA)" në Laboratorin Kombëtar të "Departament Homeland Security" në Idao Falls, USA.

Trajnimi, i organizuar në laboratorë me pajisje industriale, i ofron pjesmarrësve një përvojë reale të sulmeve dhe mënyrës së mbrojtjeve së këtyre sistemeve, të ndarë në ekipe Blue Team dhe Red Team, duke përdorur mjete si Kali Linux dhe Security Onion.

Pjesëmarrja aktive në trajnimet e zhvilluara nga CISA i shërben AKCESK për rritjen e kapaciteteve teknike dhe bashkëpunimin në ekip gjatë menaxhimit të një incidenti kibernetik në Sistemet Idustriale të Kontrollit.

Ngritja e kapaciteteve në fokus të "Balkan CyberSecurity Days"

Në kuadër të objektivave strategjikë në terma të ngritjes së kapaciteteve, AKCESK mori pjesë në trajnimin " Balkan Cybersecurity Days të zhvilluar në Ohër, në datat 16-18 maj.

Qëllimi i trajnimit ishte rritja e kapaciteteve mbi njoftimin dhe mitigimin ndaj sulmeve kibernetike, teknikat me te mira në *threat intelligence,* mbrojtja nga sulmet DDoS dhe sulmet phishing.

Pjesëmarrja në trajnim i mundëson AKCESK rritjen e kapaciteteve njerëzore në terma të hetimit digjital dhe mbrojtjes së sistemeve nëpërmjet teknikave të avancuara të analizës së sigurisë.

Phishing Alert për sektorin e turizmit

Sulmet kibernetike më të shpeshta në sektorin e turizmit, janë ato drejt hotelerisë.

Si ndodh kjo?

Individët apo grupet e individëve që organizojnë sulme të tilla, fillimisht sillen si klientë. Ata përdorin platforma të ndryshme si Booking për kryer "rezervimet" për hotele të ndryshme.

Më pas duke pretenduar se janë alergjikë i dërgojnë hoteleve në email apo nga Booking file të infektuar.

KUJDES! MOS HAPNI FILE QË JU DËRGOJNË KLIENTËT!

Pasi kanë infektuar kompjuterin e hotelit, hacker-at marin akses tek emailet e hoteleve ose llogaritë e tyre në Booking dhe sigurojnë aty numrat e kontaktit të klientëve, të cilët kanë bërë rezervime.

Hacker-at i shkruajnë klientëve në Whatsapp me numra të ndryshëm 1 përdorimësh, të cilët sigurohen në internet, duke i dërguar një link ku pretendohet se duhet të konfirmohet rezervimi, por faktikisht ata aksesojnë të dhënat e kartave të kreditit të këtyre klientëve.

Këto sulme kibernetike quhen "phishing" dhe janë duke u përhapur gjithnjë e më shumë në mbarë botën.

KUJDES! MOS BINI PRE I TYRE!

MBRONI VETEN DHE KLIENTËT TUAJ!

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