WEEKLY BULLETIN

15-19 MAY 2023

Quote of the week

"Cybersecurity is much more than an IT matter"

Content:

Important security update for Wordpress

A recently discovered vulnerability in the Wordpress platform, identified as CVE-2023-30777, is being actively exploited by attackers.

The XSS (Cross-site scripting) vulnerability allows access to sensitive information and escalation of privileges on infected sites built with WordPress.

WordPress site administrators are advised to immediately apply the Advanced Custom Fields updates to versions 5.12.6 and 6.1.6, to protect against scanning and exploit activities.

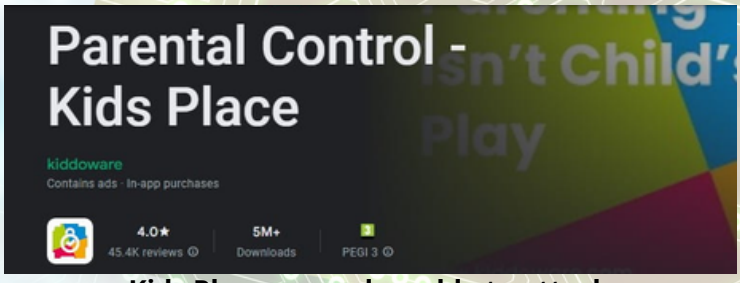
Link: Read more

CyberAttack on personal data at the US Department of Transportation

The US Department of Transportation (USDoT) reported that the personal data of 237,000 former and current employees was exposed in a cyber attack. The attack did not affect any other systems and was isolated in time from the systems of administrative functions.

Federal agencies and their employees have been the target of cyber attacks before.

Link: Read more



Kids Place app vulnerable to attacks

Researchers have discovered five vulnerabilities in the Kiddoware Kids Place Parental Control app for Android.

The vulnerabilities allow attackers to upload infectious files to children's devices, steal user credentials, and allow children to bypass restrictions placed on the app without parents noticing.

Users are advised to update to the latest version 3.8.50 on Google Play immediately to protect security and privacy.

Link: Read more

PATCHING ALERT

Security updates from Apple

Apple has released security updates for 3 WebKit Zero-Day vulnerabilities that could affect iPhones and Macs.

Vulnerabilities, which could lead to the exposure of personal information, have been resolved in the operating systems iOS 16.5 and iPadOS 16.5.

AKCESK recommends all Apple users to install the updates.

Link: Read more

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

WEEKLY BULLETIN

15-19 MAY 2023

Content:

- **Protection from cyber attacks and increased security for Industrial systems**
- **Capacity building in focus of "Balkan CyberSecurity Days"**
- **Phishing Alert for tourism sector**

Protection from cyber attacks and increased security for Industrial systems

In the framework of raising the technical capacities of Critical Infrastructures, which operate on Industrial Systems, AKCESK participated in the ICS 301L training developed by the "CyberSecurity and Infrastructure Security Agency (CISA)" at the National Laboratory of the "Department of Homeland Security" in Idao Falls , USA.

The training, organized in laboratories with industrial equipment, offers participants a real experience of attacks and how to defend these systems, divided into Blue Team and Red Team , using tools such as Kali Linux and Security Onion.

Active participation in the trainings developed by CISA serves AKCESK to increase technical capacities and team cooperation during the management of a cyber incident in Industrial Control Systems.

Capacity building in focus of "Balkan CyberSecurity Days"

Within the framework of strategic objectives in terms of capacity building, AKCESK participated in the "Balkan Cybersecurity Days" training held in Ohrid, on May 16-18.

The purpose of the training was to increase the capacities on notification and mitigation against cyber attacks, the best techniques in threat intelligence, protection from DDoS attacks and phishing attacks.

Participation in the training enables AKCESK to increase human capacities in terms of digital investigation and systems protection through advanced security analysis techniques.

Phishing Alert for tourism sector

The mos frequent cyber attacks in the tourism sector are those towards the hotel industry

How does that happen?

Individuals or a group of individuals who organize such attacks initially act as clients. They use different platforms like Bookings to make "booking" for different hotels

Then pretending that they are allergic, they send infected emails or Booking files to the hotels.

BE AWARE! DO NOT OPEN FILES SENT TO YOU BY CLIENTS!

After infecting the hotel's computer, the hackers gain access to the hotels' emails or their Booking accounts and obtain the contact numbers of costumers who have made reservations there.

Havkers write to costumers on Whatsapp with various one-use numbers, which are secured on the Internet, sending them a link claiming to confirm the booking, but in fact they access the credit card detalis of these customers.

These cyber attacks are called "phishing" and they are spreading more and more around the world.

BE AWARE! DO NOT FALL THEIR PRAY!

PROTECT YOURSELF AND YOUR CLIENTS!

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