

WEEKLY BULLETIN

5-9 FEBRUARY 2024



Quote

"As cybersecurity leaders, we have to create our message of influence because security is a culture and you need the business to take place and be part of that security culture."

Britney Hommertzhaim

of the week

Content:

- Conference: "A safer cyber space for children"
- NAECCS in strengthening cyber security capacities



Conference: "A safer cyber space for children"

In the framework of the "International Safe Internet Day", NAECCS in cooperation with ASHDMF, organized the Conference on "A safer cyberspace for children". This conference was organized in the premises of the Prime Minister's Office, in the Center for Openness and Dialogue (COD), on February 6, 2024, where the two heads of institutions, Mr. Igli Tafa and Mrs. Alma Tandili signed the cooperation agreement between the two institutions responsible for meeting the objectives for the protection of children and young people online. The institutions committed to implement a common action plan throughout the year 2024, to carry out various activities and awareness campaigns.

At the Conference, a proactive discussion was held with children and young people invited from two schools in Tirana, the Kosova middle school and the Sami Frashëri High School, on the many risks they face in the digital space, how to protect and report cases of abuse or the distribution of images with inappropriate content, as well as the measures that must be taken by the institutions responsible for raising awareness and protecting children.

At the Conference, Mrs. Bora Muzhaqi Minister of State for Youth and Children, Mrs. Clarisse Pasztory, the Deputy Head of the OSCE Presence in Albania held a speech, as well as representatives from various institutions such as the Embassy of Netherlands, the Swiss Embassy, the State Police, the Municipality of Tirana, Alo 116 111, AKEP, AMA, Risi Albania, the organization Save the Children, etc., who shared their experiences regarding cases where children have been the subject of abuse, bullying or victims of illegal content material distributed online.



NAECCS in strengthening cyber security capacities

In the framework of the creation of a safe cyber ecosystem for business in Albania, on January 31, 2024, the "Cybersecurity Hackathon" activity was organized with participants from the business sector, under the direction of the Albanian Trade Union with the support of NAECCS and the Risi Albania project, implemented by Helvetas.

Considering the digitization of processes and the evolution of technologies that businesses use as well as the increase in the number of cyber security threats, the development of human and technical capacities in this area is essential to guarantee the security and continuity of business operations. This activity, organized in the format of a cyber training, created the opportunity for IT and cyber security experts of businesses to test and expand their knowledge under the guidance of NAECCS professional trainers. The cyber training focused on the implementation and management of simulated cyber attacks, with the aim of developing defensive tactics for the main business systems in Albania.

Deputy Director of NAECCS, Mrs. Floreta Faber, in her welcoming speech, expressed gratitude for the cooperation with RISI Albania in organizing joint activities and emphasized the importance of public-private cooperation for addressing cyber security challenges in the country. The key role of NAECCS was also underlined, to provide continuous support and cooperation to businesses and all critical sectors in Albania, for strengthening cyber security at the national level.



WEEKLY BULLETIN

5-9 FEBRUARY 2024



Quote

"As cybersecurity leaders, we have to create our message of influence because security is a culture and you need the business to take place and be part of that security culture."

Britney Hommertzhaim

of the week

Content:

- A new version of the malware is discovered: Android XLoaderence
- Hyundai -data breach
- JetBrains warns of a new vulnerability
- Android - patching alert

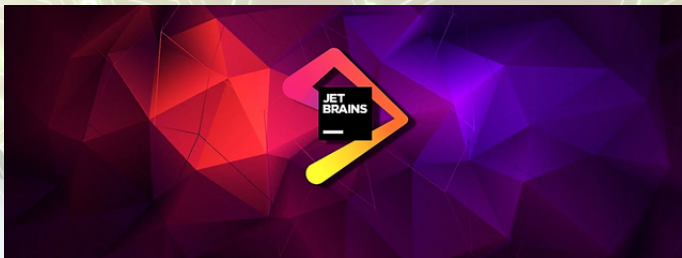


A new version of the malware is discovered: Android XLoader

A new version of the XLoader Android malware that runs automatically on the devices it infects has recently been discovered by security researchers.

Researchers report that recent variants of XLoader demonstrate the ability to activate automatically after installation. This allows malware to run stealthily in the background and collect sensitive user information. McAfee researchers suggest using a security product that can scan the device and root out these threats.

[Link: Read more](#)



JetBrain warns of a new vulnerability

JetBrains warns customers to update their TeamCity On-Premises servers against a critical vulnerability, which could allow attackers to gain administrator privileges.

Identified as CVE-2024-23917, this critical vulnerability affects all versions of TeamCity On-Premises and can be exploited in remote code execution (RCE) attacks.

All TeamCity On-Premises users are advised to update their servers to version 2023.11.3 to eliminate the vulnerability.

[Link: Read more](#)



Hyundai- data breach

Car manufacturer Hyundai Motor Europe has suffered a Black Basta ransomware attack, in which threat actors claim to have stolen three TB of corporate data.

While it is not known what data was stolen, the names of the files accessed indicate their connection to various departments in the company, including legal, sales, human resources, accounting, IT and management.

[Link: Read more](#)

PATCHING ALERT



Android- patching alert

Google released the Android security patch in February 2024 to address 46 vulnerabilities, including a critical remote code execution vulnerability identified as CVE-2024-0031.

Google released Android security patch level 2024-02-01 and 2024-02-05 to fix the issues found.

Users should apply security patches as soon as software updates are available to them.

[Link: Read more](#)

