WEEKLY BULLETIN
26-30 JUN 2023

Quote of the week

"No technology that is connected to the Internet is unhackable." - Abhijit Naskar

AKCESK participates in the Cyber Week activity in Tel Avivc

Within the framework of the cooperation agreement with Israel, AKCESK actively participated in the "Cyber week" activity, which is a large annual international cyber security event, organized every year at Tel Aviv University. Over the past eight years, Cyber Week has been internationally recognized as one of the world's leading cyber security events.

In one of the panels of this activity, the Crystal Ball Platform was presented, a platform involving countries and partnerships that enables the analysis and sharing of information in an interactive, fast, secure and easy way between countries on cyber defense issues. What was evident both in terms of technology and interoperability in the field of cyber security was that common cyber security challenges are overcome by working together, sharing knowledge, experiences and technologies for better and faster protection.

During this week, the Deputy General Director of AKCESK held a series of meetings with representatives of counterpart institutions from other participating countries, as well as with industry, in terms of increasing cooperation between countries and implementing new technological solutions.

High-Level Cybersecurity Conference
TOWARDS A RESILIENT CYBERSPACE IN THE WESTERN BALKANS
Brussels 28-29 June 2023

Regulatory Dialogue between the European Union and the Western Balkans at the Cyber Security Conference in Brussels

On June 30, 2023, the second meeting with the European Commission on the "Regulatory Dialogue between the European Union and the Western Balkans" was organized in Brussels. Also, on June 28-29, 2023, the "Regional Cooperation in Case of Potential Cyber Incidents" workshop took place within the Berlin process, to strengthen cyber security capacities in the Western Balkans region.

During its participation, AKCESK participated in 2 panels:

1. How Regional Cooperation Strengthens Cybersecurity – Opportunity and Approaches
2.EU Cyber Ecosystem: Lessons Learned and Opportunities for the Western Balkans.

In both panels, issues on the importance of regional and international cooperation were discussed, as well as what were the lessons learned on the problems encountered, best practices and plans for raising the levels of cyber security at the regional level.

Meeting with the European Commission

During the meeting with the representatives of the European Commission, the representatives of the EC discussed topics such as:

- Open Data Directive - Non localization, free flow of non personal data
- Data Governance Act
- Cybersolidarity Act
- EU Cybershield

AKCESK made a presentation of the work done by the Authority on:

- Alignment of the legal framework on cyber security in accordance with the requirements of the European directives NIS1 and NIS2,
- Improving the legal framework on trusted services with eIDAS,
- Support on ENISA methodologies, regulations and directives,
- Changes in strategic plans in cyber governance issues,
- Increasing technical capacities on cyber security
- Increasing regional and international cooperation
- Increasing cooperation with private companies.

At the end of the speech, AKCESK also requested the increase of cooperation and assistance of the European Commission on the improvement of the legal and procedural framework in full compliance with EU requirements and standards.

WEEKLY BULLETIN

26-30 JUN 2023

Quote of the week

"No technology that is connected to the Internet is unhackable." - Abhijit Naskar

Content:

- A critical security vulnerability in WordPress plugin, exposes user accounts
- The Jumsec company identifies the delivery of a malware in Microsoft Teams
- MOVEit - Data breach
- Goole Chrome 114- Patching Alert

A critical security vulnerability in WordPress plugin, exposes user accounts

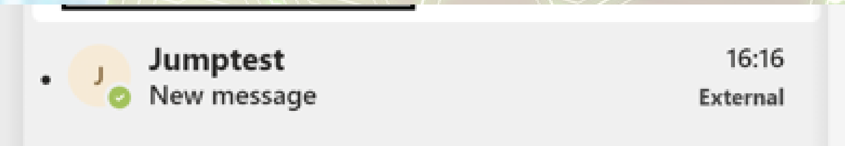
About 200,000 WordPress websites are at risk of ongoing attacks exploiting a critical security vulnerability.

The vulnerability identified as CVE-2023-3460 can be exploited by unauthenticated attackers to create new user accounts with administrative privileges, giving them the power to take full control of the affected sites.

The issue came to light after reports surfaced of rogue admin accounts being added to affected sites, prompting maintainers to release partial fixes in versions 2.6.4, 2.6.5 and 2.6.6. A new update is expected to be released in the coming days.

It is also recommended to audit all admin-level users on websites to determine if unauthorized accounts have been added.

[Read more]



Jumptest
New message
16:16
External

The Jumsec company identifies the delivery of a malware in Microsoft Teams

Researchers from security services company Jumpsec have identified a method to send malware through Microsoft Teams.

The attack methodology relied on bypassing application restrictions on externally sourced documents.

This communication bridge, in addition to being used in Social Engineering and phishing acts, also enables the sending of a malicious payload to the target's address.

Companies and Institutions that use Microsoft Teams and do not regularly communicate with external users are advised to disable this option in the Microsoft Teams Admin Center.

[Read more]

Cyberattacks expose sensitive data about public school students and staff

A cyberattack has exposed sensitive data about about 45,000 New York Public School students — as well as Department of Education staff and service providers.

The documents accessed include student evaluations, and the exposed data includes social security numbers and dates of birth.

Cyber attackers began targeting a previously unknown vulnerability in the popular file transfer software MOVEit allowing the infection of 150 organizations, which compromised the personal data of over 16 million individuals.

Until now, none of the data stolen from public school students has been published.

[Read more]

PATCHING ALERT

Chrome 114 critical patch alert

Google recently announced a new Chrome 114 update that fixes a total of four vulnerabilities including three critical bugs reported by external researchers.

The critical vulnerabilities, which cause memory corruption that Google has been struggling with in both Chrome and Android, can lead to arbitrary code execution, data corruption, or a denial of service.

The latest Chrome updates appear as version 114.0.5735.198 for macOS and Linux and as versions 114.0.5735.198/199 for Windows.

AKCESK recommends all Google Chrome users to perform the necessary updates

[Read more]