

CYBER SECURITY NEWS BULLETIN



July 2023

Content:

- Cyber Defense Strategy Development Workshop
- Western Balkans: Transatlantic and Regional Cooperation - Building Strong Alliances
- AKCESK Participates in the Training for Response to Cyber Incidents for Critical Information Infrastructures
- Cyber Crisis Governance Workshop



Cyber Defense Strategy Development Workshop

On July 18-21, 2023, the Security Governance Institute of the US Defense Security Cooperation Agency organized the "Cyber Defense Strategy Development" workshop near the premises of the General Staff of the Armed Forces.

Participants in this workshop were representatives from the Ministry of Defense, the General Staff of the Armed Forces, the Military Cyber Security Unit, the National Agency of the Information Society and AKCESK.

The purpose of the workshop was the development and implementation of the cyber defense strategy, to support the mission and harmonize the priorities, structures, decisions and objectives of the Ministry of Defense, for the protection of the Albanian cyberspace.



Western Balkans: Transatlantic and Regional Cooperation - Building Strong Alliances

On July 13 in Washington, D.C, the Western Balkans Conference: Transatlantic and Regional Cooperation - Building Strong Alliances was organized.

The conference brought together important representatives, with the aim of regional cooperation, which is essential for the countries of the Western Balkans in the progress of the process of stabilizing the association in the EU.

During the session "Cyber Security in the Western Balkans: Meeting the Challenges", Albania, represented by the General Director of AKCESK Mr. Igli Tafa, presented the security challenges recalling the attack of a year ago directed at Albania, in which two main terms were adopted: technological terms where the focus has been the increase of technological capacities as well as strategic terms where the focus has been the raising of human capacities.

Also, following the discussions of this session, the head of AKCESK emphasized the support of strategic partners and the importance of continuous cooperation to deal with critical situations in a stable manner.

The conference continued the discussions by addressing the challenges, ongoing cyber attacks on public and private institutions and individuals and what are the appropriate measures to be taken in strategic terms and international cooperation.



AKCESK Participates in the Training for Response to Cyber Incidents for Critical Information Infrastructures

In the framework of raising the technical capacities of Critical Infrastructures, the National Authority for Electronic Certification and Cyber Security participated in the four-day training developed by USEA and Catalisto together with the assistance of USAID in Tirana. The focus of the program was the deepening of advanced knowledge in the management of cyber incidents in public and private infrastructures in Albania, as well as the evaluation of the implementation of security measures based on the most recognized international standards.

Active participation in this training serves AKCESK directly in creating sustainable capacities to address potential crises through strengthening strategies, innovation and cyber security



Cyber Crisis Governance Workshop

In the framework of the development of the capacities of information infrastructures, AKCESK in cooperation with CRDF Global and C3I organized the workshop on "Governance of the cyber crisis". The purpose of the workshop was to strengthen crosssectoral cooperation in terms of cybercrisis governance at the national level, through dedicated fictitious scenarios.

CYBER SECURITY NEWS BULLETIN



Content:

- Albania supports the approval of the OEWG's Annual Progress Report at the UN
- Apple releases an emergency update to address a bug in iOS and macOS
- ISA gives US civilian agencies until August 1 to fix four Microsoft vulnerabilities
- Microsoft - Patching Alert



Albania supports the approval of the OEWG's Annual Progress Report at the UN

The fifth session of the "Open-Ended Working Group (OEWG) On security of and in the use of information and communications technologies" developed its work on July 24-28, 2023 and concluded with the approval of the Annual Progress Report. Progress report represents a guide to the future work of the OEWG and reflects on the dynamic landscape of threats in the cyber ecosystem.

Albania, represented by the Permanent Mission to the UN and the Director of AKCESK Mrs. Edlira Gjollëshi, after contributing to the drafting of the Program of Action and the active role in the fourth session of the OEWG held on March 6-10, supported the approval of the Annual Progress Report, considering it as a necessary tool for the future work of the OEWG.

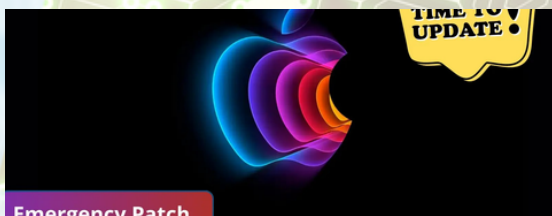
Progress report proposes concrete steps to advance peace and security in cyberspace, reflecting recent developments in the field of cyber security in the context of international security. AKCESK, in the capacity of the responsible authority in the field of cyber security at the national level, continues to follow international discussions in the field, in full coordination with the structures of the line ministry and the mission of Albania in international organizations.



CISA gives US civilian agencies until August 1 to fix four Microsoft vulnerabilities

The Cybersecurity and Infrastructure Security Agency (CISA) has given US federal civilian agencies until August 1 to resolve four serious zero-day vulnerabilities announced as part of Microsoft's monthly Patch Tuesday release. The inclusion of four vulnerabilities — CVE-2023-32046, CVE-2023-32049, CVE2023-35311, CVE-2023-36874 — in the CISA catalog means the vulnerabilities are already being exploited by hackers. The four Microsoft vulnerabilities mentioned are among more than 130 announced by the tech giant on Tuesday. Microsoft confirmed that the vulnerabilities were being exploited and affected all versions of Microsoft Outlook from 2013 onwards. In addition to Microsoft's announcements, several other companies, including Apple, Google, SAP, Fortinet, Adobe and Cisco, published advisories about their vulnerabilities.

[Read more](#)



Apple releases an emergency update to address a bug in iOS and macOS

Apple has just released an emergency update to its users to fix the vulnerabilities discovered in the security systems of iOS and MAC. The vulnerability was discovered in Apple's WebKit browser engine and allows attackers to get arbitrary code execution on target devices by tricking users into opening websites with maliciously crafted information. iOS and MAC users make the necessary updates as soon as possible and keep the automatic updates option enabled on their devices.

AKCESK recommends all apple users to install the necessary updates

[Read more](#)



Microsoft - Patching Alert

The new release of Microsoft security updates addresses 132 security vulnerabilities in products, of which 6 are zero-day vulnerabilities.

AKCESK recommends all users to install the necessary updates.

[Read more](#)