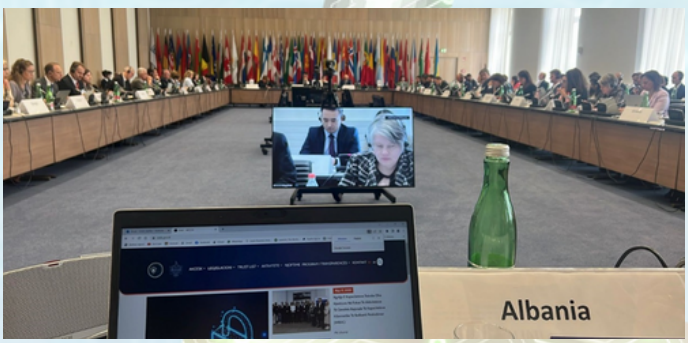
WEEKLY BULLETIN
12-16 JUN 2023

Quote of the week

"Technology trust is a good thing, but control is even better"

Content:



AKCESK participates in the OSCE activity on Confidence Building Measures

Confidence-building measures (CBM) are an integral part of the OSCE's comprehensive approach to security, which promote dialogue and emphasize cooperative solutions to common challenges. CBMs aim to reduce tensions, prevent conflicts and promote stability and security among OSCE member states.
In this context, as an active part of the OSCE, an invitation was sent to Albania for participation on June 13-15, where participants were representatives of the Ministry of Foreign Affairs and the technical point of contact for the OSCE from the National Authority for Electronic Certification and Cybersecurity, in meetings such as below:

-Informal Working Group created by PC Decision no. 1039 (IWG) on 13 June.

During the first day, the agenda consisted of preliminary discussions on the implementation of CBM 12. Participating states, on a voluntary basis, shared information and facilitated interstate exchanges in various formats, including round tables, at the regional and/or sub-regional level. To the National Authority for Electronic Certification and Cybersecurity, report all achievements made under each CBM. All achievements made by the Authority in accordance with CBM 12 were also reflected.
- Consultations on the OSCE Program of Action to advance the responsible behavior of states in the use of information and communication technologies in the context of international security (PoA) on 14 June.

During the second day, the purpose of the consultation was to provide an opportunity for participating states to share their views on the scope, content and modalities of the OSCE program with a view to further consideration of this proposal by the General Assembly. The consultations aimed to enrich the General Assembly's consideration of a future United Nations program of action by fostering a deeper understanding of regional and sub-regional perspectives. Albania gave its contribution, in accordance with the previous PoA meeting, reflecting the statement prepared by the National Authority for Electronic Certification and Cyber Security, on the contribution of the Directorate of Cyber Security Governance, Control and Strategic Development and the Directorate of Cyber Security Analysis as well as in cooperation with the Ministry for Europe and Foreign Affairs.
- The annual meeting of national contact points appointed in accordance with the OSCE Confidence-Building Measure (CBM) No. 8, on June 15, 2023, where our country's goals for the future related to activities and cooperation at the national, regional and international level were reflected.

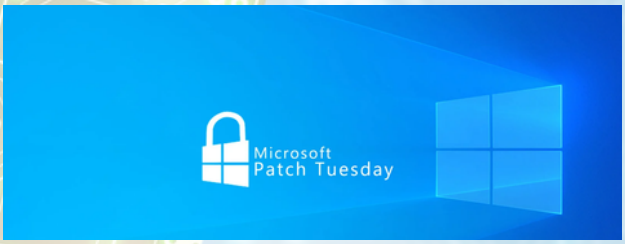
The OSCE Secretariat, as one of the organizations active and involved in cyber security issues, also emphasized the importance of Albania's participation in the OEWG (Open-Ended Working Group on Security) and the United Nations in order to properly address all the achievements and progress of Albania in matters of cyber security, which is a priority on the agendas of all UN countries, in these important international organizations.

Known threat groups identified as: Anonymous Sudan, REvil and KillNet, in June 2023 against Western financial systems

According to a June 14, 2023 Telegram post claiming to represent the threat groups Anonymous Sudan, REvil, and KillNet warned of plans to launch devastating cyber attacks against Western financial targets, including the SWIFT system, the Federal Reserve and the European Central Bank in the next two days. According to the post the cyber attack will not only be a DDoS attack, but it will be "the most powerful cyber attack in the history of the world" and that many European banks will be attacked.

As a result of ongoing research into cyber attacks, it is hinted that these attacks are DDoS attacks focused on client applications, where we may see some limited outages on some websites and some clients may not be able to access some websites.

PATCHING ALERT



Microsoft releases new updates for 78 vulnerabilities

Microsoft recently updated 78 vulnerabilities, including 38 remote code execution vulnerabilities.

While thirty-eight code bugs were fixed, Microsoft listed only six vulnerabilities as 'Critical', including denial of service attacks, remote code execution and privilege violation.

The vulnerabilities have been patched by the Microsoft team.
AKCESK recommends all users to use the updated version

Link: Read more

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