WEEKLY BULLETIN
22-26 JANUARY 2024

Content:

- **NAECCS holds a meeting with Financial Institutions**

- **HPE - data breach**

- **Apple - patching alert**

NAECCS holds a meeting with Financial Institutions

The cyber events in which Albania is going through recently, gathered at a discussion table on January 23, 2024, NAECCS and the senior leaders of the institutions of the financial sector.

At the meeting, the National Coordinator for Cyber Security, Mr. Igli Tafa emphasized the importance of the role of investments in this sector of critical infrastructures for increasing cyber security. The attendees got acquainted with the necessity of strengthening and cyber protection of institutions by focusing on several steps:

Investments in Technology – the need to use the latest cyber defense technologies to protect customer information and data. Operational Measures – raising the daily security standards of the institution from the operational and administrative side according to NIST or ISO 27001 references.

Managerial Level – the role of leadership in the obligation of the institution to invest in raising the awareness of the staff in the framework of cyber security, in determining the budget in the field of cyber security as well as in determining the cyber risk on an ongoing basis.

Increase of Capacities – Investment in the professional growth of experts and the coverage of identified vacancies in the field of cyber security.

The meeting emphasized the need to increase cooperation between NAECCS and the financial sector to share as much information as possible and to take appropriate measures, at the right time, that ensure a safe cyber ecosystem. The need for a continuous and active approach, in concrete cooperation, to address cyber challenges in the future was emphasized there.

NAECCS requested that the financial sector coordinate the work with concrete actions for the implementation of increased security measures for 2024.

HPE - data breach

Hackers with links to the Kremlin are suspected to have infiltrated information technology company Hewlett Packard Enterprise's (HPE) cloud email environment to exfiltrate mailbox data.

The threat actor accessed and extracted data starting in May 2023 from a small percentage of maliboxes belonging to individuals in cybersecurity, businesses, etc.
HPE, however, emphasized that the incident has not had any material impact on its operations to date.

Read more

PATCHING ALERT

Apple - patching alert

Apple has recently released security updates to address a zero-day vulnerability that has been actively exploited by attackers.
The vulnerability identified as CVE-2024-23222 is an issue in the WebKit browser engine that can be exploited by a threat actor to achieve arbitrary code execution.

The tech giant said the issue was fixed with improved controls.

Read more