# WEEKLY BULLETIN
## 9-13 OCTOBER 2023

**Quote**

*"Technology, like art, is a soaring exercise of the human imagination.*

***Daniel Bell***

*of the week*

**Content:**

- **Security Policies and Crisis Management for the Health Sector.**

- **AKCESK participates in Cyber Week Regional training**



### Security Policies and Crisis Management for the Health Sector.

In the framework of the trainings that will be organized by NAECCS for the period October-December 2023, on October 11-12, the training on "Cyber Security Policies and Crisis Management" for the Health Sectors took place.

During this two-day training, presentations were made regarding Legislation, Strategy, Policies and Cyber Governance needs, as well as 3 Table Top Exercises for the management of Cyber incidents and crises, Simulating a "Phishing" attack as well as an infection scenario case from Malware, a Cyber Drill was also organized where there were concrete exercises on incident management. During the discussions, the importance of improving coordination, cooperation and information exchange on the analytical and reaction capacities of the health sector entities related to cyber security incidents was emphasized.
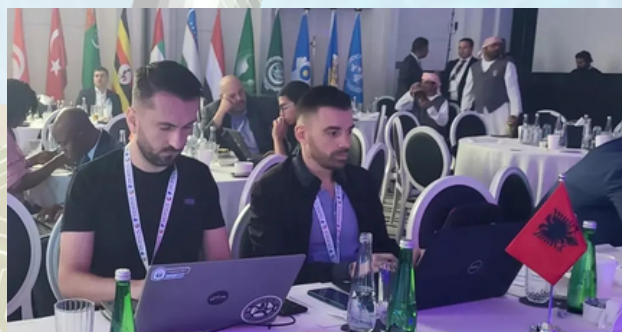


### AKCESK participates in Cyber Week Regional training

By invitation of the United Arab Emirates, NAECCS participated in Cyber Week Regional. In the first two days, a cyber drill Cyber Drill excercise was organized where there were representatives from 70 nations.

The representatives of NAECCS represented Albania decently and were classified as follows:

**Scenario 1 - Hacked and Crypto Mining Web Apps Analysis Log: First place out of 30 participating countries**

Scenario 2 – Defense Tactics for Cyber Security (12th Place);
Scenario 3 – DFIR (9th place);
Scenario 4 – Cyber threat intelligence (there were no classifications);
Scenario 5 – CPX Ransomware Technical (11th place) ;
Scenario 6 - CPX Ransomware MAnagement (there were no classifications);
Scenario 7 - Threat Emulation Lead (8th Place);
Scenario 8 – OSINT ( 5th Place);

# WEEKLY BULLETIN
## 9–13 OCTOBER 2023

**Content:**

- A new threat on the horizon: the APT Grayling Group
- Over 17,000 WordPress websites compromised by Balada Injector
- CISA reports vulnerabilities and misconfigurations exploited by Ransomware
- Google Chrome - patching alert

## A new threat on the horizon: the APT Grayling Group

An unidentified APT group, known as Grayling, has targeted a variety of organizations spanning Taiwan's manufacturing, IT and biomedical sectors.

For organizations aiming to defend against such threats, keen vigilance over network anomalies and rigorous patch management, especially for known vulnerabilities like CVE-2019-0803, would be imperative.

**Read more**

## Over 17,000 WordPress websites compromised by Balada Injector

More than 17,000 WordPress websites were recently compromised with a malware known as Balada Injector.

9,000 of these websites are believed to have been infiltrated using a recently discovered vulnerability identified as: CVE 2023-3169 which can be exploited by unauthenticated users to perform XSS (cross-site scripting) attacks.

**Read more**

## CISA reports vulnerabilities and misconfigurations exploited by Ransomware

US cybersecurity agency CISA is stepping up its efforts to prevent ransomware attacks by making it easier for organizations to learn about the vulnerabilities and misconfigurations exploited in these attacks.

As part of its Ransomware Vulnerability Warning Program (RVWP) launched in March, the agency has released two new information resources to help organizations identify and eliminate security vulnerabilities known to be exploited by ransomware groups.

**Read more**

## PATCHING ALERT

### Google Chrome - patching alert

Google recently released Chrome 118 with updates for 20 vulnerabilities, including a critical vulnerability.

The Internet giant does not mention any of these vulnerabilities being exploited in malicious attacks.
The updated version of Chrome is 118.0.5993.70 for macOS and Linux, and as version 118.0.5993.70/.71 for Windows.

AKCESK advises all Google users to perform the necessary updates.

**Read more**