WEEKLY BULLETIN
20-24 NOVEMBER 2023

Quote of the week

"At the end of the day, the goals are simple: safety and security."

Content:

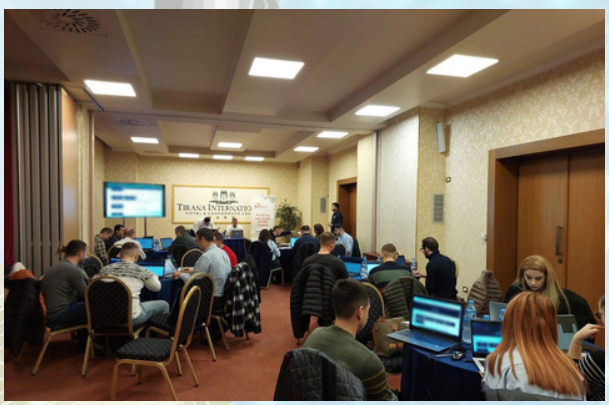
Capacity building, essential for the protection of critical and important information infrastructures

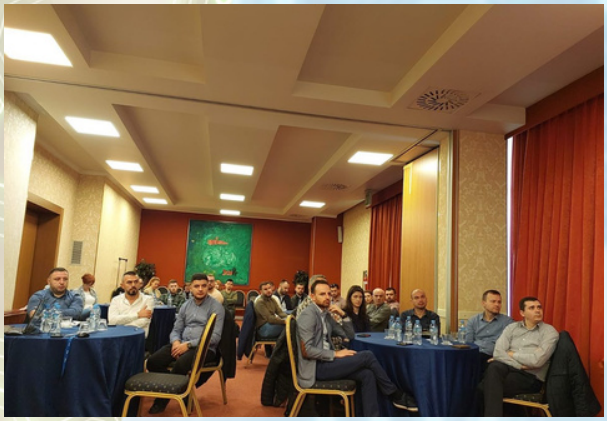
NAECCS, focused on increasing the level of cyber security in information infrastructures at the national level, supports the Operators of Critical and Important Information Infrastructures, to increase their professional and technical capacities.

Considering the increase of capacities as one of the essential pillars for the protection of information infrastructures, NAECCS continuously offers help and support to all operators of these infrastructures. In this line, the activity of 23-24 November with the financial/banking sector was developed with the support of our partner Risi Albania/Helvetas and the valuable contribution of the Authority's experts.

The two-day activity focused on the development of various TTX scenarios, dedicated to this sector, and the participants were involved in the Cyber Drill exercise, showing their skills in solving cyber incidents based on the relevant procedures.

NAECCS is always attentive to the use of new technologies and techniques, following international standards in the field of cyber security and ready to support all groups of society, for the construction of a sustainable cyber ecosystem in Albania.





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

WEEKLY BULLETIN

20-24 NOVEMBER 2023

Quote of the week

"At the end of the day, the goals are simple: safety and security."

Content:

Exploitation of a critical Windows Defender vulnerability becomes public

Threat actors are actively exploiting the zero-day vulnerability identified as: CVE-2023-36025 in Windows SmartScreen.

CVE-2023-36025 is the third zero-day vulnerability in SmartScreen that Microsoft has disclosed so far this year. In February, researchers at Google found a threat actor exploiting a previously unknown SmartScreen vulnerability to install Magniber ransomware on target systems. Microsoft identified the vulnerability as CVE-2023-24880 and released a patch for it in March.

Read more

The number of victims of the massive MOVEit attack rises to over 2,600 firms, 77 million people

According to researchers, 2,620 organizations and more than 77 million individuals have been affected, receiving notifications that their information was accessed, after the Russian Clop ransomware gang exploited a vulnerability to steal various files.

Avast Antivirus is among the new victims, which recently revealed that fraudsters had access to some "low-risk personal information of customers".

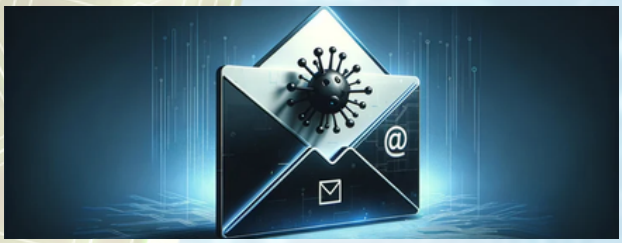
Read more

The identified vulnerability in Sophos Web Appliance is actively exploited

CISA has added three vulnerabilities to its catalog of actively exploited vulnerabilities, among them a critical vulnerability (CVE-2023-1671) in the Sophos Web Appliance.

A public PoC exploit for CVE-2023-1671 has been available since late April, as well as a script that can be used by defenders to scan for vulnerable devices on their network.

Read more



A new malware identified as WailingCrab is spreading rapidly through emails

The attack chain begins with an email containing a PDF attachment that contains URLs that, when clicked, download a JavaScript file designed to load the WailingCrab malware.

Actively maintained by its operators, this malware has been observed to include features that prioritize stealth and allow it to resist analysis efforts.

Read more

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