WEEKLY BULLETIN
22-26 MAY 2023

Quote of the week

"Amateurs hack systems, professionals hack people."

Content:

Microsoft 365 phishing attacks use encrypted RPMSG messages

Cyber attackers have devised a new method to carry out targeted phishing attacks. It is via using encrypted RPMSG(Restricted permission message files) attachments transmitted through compromised Microsoft 365 accounts. This technique aims to bypass email security gateways.

RPMSG's authentication requirements are now being exploited to trick targets into handing over their Microsoft credentials using fake login forms.

To help prevent Microsoft 365 accounts from being compromised, users are advised to enable Multi-Factor Authentication (MFA).

Read more

A new malware creates backdoors on Microsoft Exchange servers.

A new PowerShell-based malware called PowerExchange was used by Iranian attackers to create backdoors on Microsoft Exchange servers.

After penetrating the server through a phishing email that contained existing malicious code, the attackers deployed a web shell called ExchangeLeech to steal user credentials.

Organizations using Microsoft Exchange servers are advised to implement strong security practices and promptly apply relevant updates to protect against threats.

Read more

Free VPN service called SuperVPN exposes 360 million user records.

Researchers recently discovered a significant data breach of a database associated with a free VPN service that contained 360 million records exposing data such as: email addresses, IP addresses, geolocation data, and server usage records.

This is not the first time SuperVPN has exposed user data, for this reason users are advised to make more informed choices to protect their online privacy and security.

Read more

PATCHING ALERT

GitLab-security update

The GitLab website dedicated to developers has released an emergency security update for a critical vulnerability identified as CVE-2023-2825.

The vulnerability exposes sensitive data such as user credentials, files and other private information, for this reason users are advised to update to version 16.0.1 to mitigate the risk.

AKCESK recommends all GitLab users to install the latest updates.

Read more

Rruga "Papa Gjon Pali II", No.3 info@cesk.gov.al

Autoriteti Kombëtar për CESK

autoriteti_kombetar_cesk

+35542221039

WEEKLY BULLETIN

22-26 MAY 2023

Content:

Cybersecurity Leadership Program

The five-day intensive training at Duke University and at Microsoft in the United States of America brought together private and public sector leaders, as well as key industry experts in the field of cyber security.

The focus of the program was to deepen advanced knowledge to meet tomorrow's challenges in the field of cyber security and mitigate the risk of these attacks.

The Cyber Security Leadership Program consisted of dedicated topics including Cyber Security and the Board, Challenges for CISOs, Data Breach Preparedness and Response, Impact of Cyber Incidents.

Technical and human capacity building with a focus on regional cooperation

On May 25-27 AKCESK participated in the 31st NISPACee Conference organized by ReSPA "The Future of Public Administration through Emerging Technologies" in Belgrade, Serbia. The purpose of this conference was the role of public administration in accordance with rapid socio-economic changes, taking into account the opportunities offered by new technologies, as well as the development of necessary services aimed at openness, transparency and participation of citizens in decision-making.

Active participation in this conference serves AKCESK directly in increasing regional cooperation, creating sustainable capacities to address potential crises through strengthening strategies, innovation and cyber security.

Threat Hunting training

In the framework of the support of the Council of Europe through the e-Governance Academy and following the activities to strengthen the capacities of the responsible staff, AKCESK in cooperation with Cybexer Technologies, organized the cyber exercise "Threat hunting", with participants from critical information infrastructures.

The training serves to increase technical capacities through cyber exercises, based on Table Top Exercise and simulations according to dedicated scenarios of cyber attacks that can affect different sectors of critical information infrastructures.

Active participation in this training serves AKCESK to increase technical capacities in order to resolve cyber incidents in Critical Information Infrastructures.

Harmonization of the legal framework with the EU, in order to strengthen cyber security at the national level

On May 25-26, the European Commission held a bilateral meeting on Chapter 20 "Enterprises and Industrial Policies", within the integration process. AKCESK, within the framework of commitments undertaken as a candidate country for EU membership, presented the developments for the harmonization of the legal framework of the field with the EU, through the draft law "On cyber security", as well as the innovative initiative for the establishment of the National Academy of Cyber Security, which aims to increase the level of cyber security through the strengthening of human capacities. The meeting reaffirms the progressive approach of the Albanian Government in terms of harmonizing policies in the field of cyber security with the EU, as well as the priority for strengthening cyber security, using the potential of scientific research, innovation and cooperation with actors of the field.

Cyber Security Assessment in Industrial Systems, ICS 401 L.

In the framework of raising the technical capacities of Critical Infrastructures, which operate on Industrial Systems, AKCESK participated in the ICS 401L training developed by the "CyberSecurity and Infrastructure Security Agency (CISA)" at the National Laboratory of the "Department of Homeland Security" in Idao Falls , USA.

The focus of this training was the assessment of Cyber Security in Industrial Systems. During the training, the participants were introduced to the CSET tool, which enables the evaluation of the Cyber Security of Industrial Systems of Critical Infrastructures as well as the evaluation of the implementation of security measures based on the most recognized international standards.

Active participation in the trainings developed by CISA serves AKCESK for increasing technical capacities and team cooperation during the management of a cyber incident in Industrial Control Systems.

Rruga "Papa Gjon Pali II", No.3 info@cesk.gov.al

Autoriteti Kombëtar për CESK

autoriteti_kombetar_cesk

+35542221039