WEEKLY BULLETIN
25-29 SEPTEMBER 2023

Quote of the week

> *"The absence of security in the initial stages of System Engineering is the single most significant cybersecurity gap and risk in modern system development"*
>
> ***Linda Rawson***

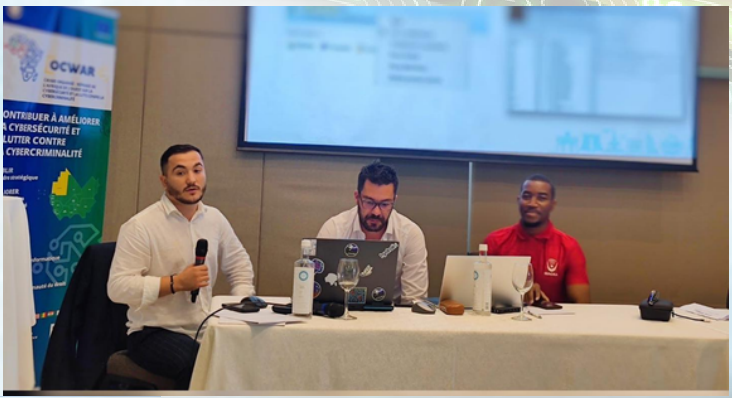
Content:

AKCESK participates in the training for regional inter-institutional cooperation CSIRT/LEA

Following the activities to increase human capacities in the field of cyber security, the National Authority for Cesk, participated in the training for inter-institutional cooperation CSIRT/Regional LEA, organized in Port Louis, Mauritius, on September 25-29, 2023, within of projects co-financed by the European Union and the Council of Europe, GLACY+ and OCWAR-C.

The aim of the training was to strengthen the CERT-LEA cooperation, with a focus on the exchange of information and the absorption of practical knowledge in technical terms such as Digital Forensics, Electronic evidences, OSINT investigation, malware analysis, bitcoin seizure, etc.

The participation of AKCESK representatives was evaluated and singled out in the group, for the contribution and dignified presentation of scenario solutions, during the Table Top Exercise.



AKCESK - 114th Member of the Global Forum of Cyber Expertise (GFCE)

Within the framework of achieving strategic objectives, in terms of strengthening human capacities in the field of cyber security, the National Authority for Electronic Certification and Cyber Security has successfully finalized the membership process in the Global Forum of Cyber Expertise.

AKCESK, as a member of the GFCE, will effectively contribute to addressing national needs, increasing cooperation and effective international coordination for capacity building, with the aim of increasing the level of cyber security at the regional and global level.

WEEKLY BULLETIN
25-29 SEPTEMBER 2023

Quote of the week

"The absence of security in the initial stages of System Engineering is the single most significant cybersecurity gap and risk in modern system development"
Linda Rawson

Content:

Cisco warns of vulnerabilities in IOS and IOS XE software after exploit attempts

Cisco is warning of attempts to exploit a security vulnerability in its IOS and IOS XE software that allows remote code execution on affected systems.

The vulnerability is identified as CVE-2023-20109 and has a CVSS of 6.6. It affects all software versions that have the GDOI or G-IKEv2 protocol enabled.

Read more

```
00000049  29 08 00 00 00 00 00 00  00 39 cf d5 a9 11 6f d1  ).......  .Y....o.
00000059  ee 97 3e 27 ab b4 c5 77  da 7d 2a 98 f0 fa ba d6  ..>'...w  .}*.....
00000069  a9 0a 1f 7e 2b 83 76 c1  62 b4 fa 37 f2 36 1d ea  ...~+.v.  b..7.6..
00000079  b6 d1 ca 28 d7 c7 13 d0  0c c8 74 19 54 11 a1 37  ...(....  ..t.T..7
00000089  4d 20 49 80 6d cd 57 dc  48 38 3e 56 36 be 6f 0c  M I.m.W.  H8>V6.o.
00000099  db de ad ad 67 20 87 d2  e6 e7 4e 10 07 17 8e 8a  ....g ..  ..N.....
000000A9  be af ed 03 ef 8c 0d 7c  b5 8f 82 eb 71 c9 fa d3  .......|  ....q...
000000B9  e3 b0 6c 10 ac 7d fb ac  d9 8c 49 35 9c 3b 0b 18  ..l..}..  ..I5.;..
000000C9  8e 24 42 19 c2 d5 23 09  ab 36 c4 07 df c1 cb f2  .$B...#.  .6......
000000D9  c8 d0 f8 90 59 4e 45 6a  e4 a6 db 43 cc 24 72 ee  ....YNEj  ...C.$r.
000000E9  82 a2 f3 3a 6d e4 46 6d  ce 10 cb f0 d3 a8 29 dd  ...:m.Fm  ......).
000000F9  6b 18 fd bf e0 37 08 04  db a2 88 25 70 f4 a9 13  k....7..  ...%p...
00000109  2f d8 a8 fb dd c1 2f 9d  cb 42 07 a4 da f4 1c fb  /...../.  .B......
00000119  ef 3e 06 c2 7c 85 86 a4  81 4c fe b4 35 b3 9f 4a  .>..|...  .L..5..J
00000129  66 f2 fa bd 63 2c 0d 5e  12 34 83 b6 ab 17 08 a6  f...c,.^  .4......
00000139  00 e4 6d 46 99 ff 6a 7f  86 84 4b 2b 8a 40 a5 75  ..mF..j.  ..K+.@.u
```

A malware identified as ZenRat targets Windows users

According to Proofpoint researchers, a new type of malware called ZenRAT has been developed to steal information from Windows systems and is distributed through the installation of fake password management packages.
ZenRAT, once installed, collects important information such as: CPU name, GPU name, operating system version, RAM or IP address and installed applications.

To mitigate such threats, it is recommended that users download software only from trusted sources and ensure the authenticity of websites.

Read more

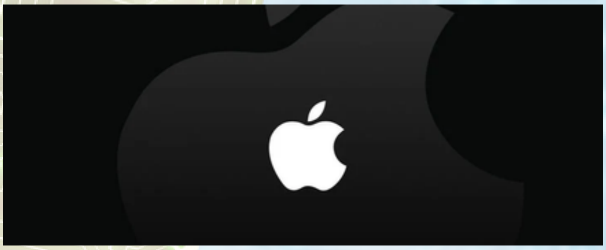
The MOVEit mass attack has claimed more than 2000 victims so far

During the month of May, the hacker group Cl0p launched a massive attack campaign exploiting a zero-day vulnerability in MOVEit software to steal data stored on file transfer servers.

Coveware, a ransomware incident response organization, estimates that the Cl0p attackers may have earned between $75 million and $100 million in ransom payments in the first few days of the massive attack campaign alone.

Read more

PATCHING ALERT



Apple - patching alert

Apple has released emergency security updates to fix three new vulnerabilities exploited in attacks targeting iPhone and Mac users, identified as CVE-2023-41991, CVE-2023-41993, and CVE-2023-41992.

The three new vulnerabilities have been patched in macOS 12.7/13.6, iOS 16.7/17.0 versions. 1, iPadOS 16.7/17.0.1, watchOS 9.6.3/10.0.1 and Safari version 16.6.1.

AKCESK recommends all users of Apple products to perform the latest updates.

Read more