Daniel Alejandro Osornio López 0244685@up.edu.mx

Preguntas

Nota: Si la practica está en inglés me parece natural responder en inglés.

1. Search the internet for SANS. From the SANS home page, click on FREE Resources. List three available resources
   - **A**: Free Resources, Free Training & Events, Podcasts & Newsletters, Free Tools, Resources by Focus Area
2. Select one of the Controls and list implementation suggestions for this control.
   - **A**: Data Protection: Use encryption and decryption techniques, implement access controls per application/user.
3. Highlight the Resources menu, select Newsletters. Briefly describe each of the three newsletters available.
   - SANS NewsBites is an annotated, semiweekly executive summary of the most recent and important cybersecurity news headlines.
   - @RISK provides a reliable weekly summary of newly discovered attack vectors, vulnerabilities with active new exploits, insightful explanations of how recent attacks worked, and other valuable data.
   - OUCH! is the world's leading, monthly security awareness newsletter designed for the common computer user. As always, translated in over 25 languages and free for the community.
4. List some recent vulnerabilities. Browse multiple recent newsletters, if necessary
   - CVE-2023-34039 - Aria Operations for Networks has an Authentication Bypass vulnerability allowing unauthorized access to its CLI.
   - CVE-2023-41359 - FRRouting FRR through 9.0 allows an out-of-bounds read in bgp_attr_aigp_valid in bgpd/bgp_attr.c during AIGP validation due to a lack of byte availability check.
5. Besides the SANS site, identify some other websites that provide recent security threat information
   - CISA
6. List some of the recent security threats detailed on these websites.
   - Zerologon vulnerability (CVE-2020-1472)
   - VMSA-2023-0026: VMware Cloud Director Appliance contains an authentication bypass vulnerability (CVE-2023-34060)
7. Step 1: Complete the following form for the selected network attack.

Name of attack: CVE-2023-34060
Type of attack: Authentication bypass
Dates of attacks: 2023-11-14
Computers/Organizations affected: VMWare
How it works and what it did:

VMware Cloud Director Appliance contains an authentication bypass vulnerability in case VMware Cloud Director Appliance was upgraded to 10.5 from an older version. VMware has evaluated the severity of this issue to be in the Critical severity range with a maximum CVSSv3 base score of 9.8.
Mitigation options:
To remediate CVE-2023-34060 follow the guidance mentioned in KB95534 in the 'Fixed Version' column of the 'Response Matrix' found below.
References and info links
https://www.vmware.com/security/advisories/VMSA-2023-0026.html

8. What steps can you take to protect your own computer?
    - **A**: Be conscious about the software and hardware on my computer, the risk every component has and update regularly to avoid falling into versions of software/drivers that are vulnerable.
9. What are some important steps that organizations can take to protect their resources?
    - **A**: The same as I will do protect my personal information, plus implementing systems that can automate, log, and prevent incidents.