Bank Network

SAHANA NAGARAJ

***Abstract*— In this research, we describe the design of a banking network, giving thorough explanations of the different components that makes the system. A thorough investigation is carried out to find the possible attack vectors that might risk the network's security. Furthermore, considering techniques for these recognized attack vectors are explained, highlighting the steps taken to strengthen the network against possible security lapses. To guarantee strong cybersecurity, the study emphasizes how crucial it is to recognize and proactively fix vulnerabilities in banking networks.**

I. Introduction

This paper reviews the architecture and security issues of bank networks, considering those devices and systems most in practical usage. It points out some vulnerabilities existing in outdated software and insecure access points that could be used to disrupt operations. The study emphasizes that the network design should be robust and able to adapt to internal processes and customer service securely, while communication and data are protected. This approach has the comprehensive integration of powerful encryption, access controls, and multiple layers of security, making regular updates, active monitoring, and quick responses possible, therefore giving a comprehensive framework in protecting banking networks against cyber threats and smooth operations in relation to industrial regulations.

II. Network Setup

Threat Modelling and Risk Assessment: The first step in creating a secure network design is classifying all the bank devices that need to be connected safely and comprehending the network architecture to safeguard the sensitive data. Card records and other personal information belonging to customers are more sensitive and may not be secure. We will have a more complete model and more information about the system. The hybrid architecture of the bank's core infrastructure combines cloud services with on-premises data centers. [1]

A central data center with different databases and Cloud-based services for disaster recovery and scalability using a software-defined wide area network (SD-WAN) to maximize branch connectivity.

The security tools that safeguard a bank network are just as important as the network architecture itself. Evaluate every security measure that is in place and find any weaknesses. Use a multi-layered security strategy in which various security systems cooperate to prevent breaches. The likelihood of a successful attack is decreased by layers of protection, but a single security tool may still leave vulnerabilities. Record all backup and failover mechanisms to guarantee that, in the event of an outage, the bank's network can continue to function securely, safeguarding private information even during interruptions.

Segmentation of networks: This is a security tactic where the network separates into different sections or categories. Segmenting the network will ensure that the attacker has the privileges even if they manage to get past all the defenses. Due to the ease of data theft, it is crucial for banks. Security is more likely when there are more layers of segmentation.

Control of Access: After segmentation is completed, we can create a strong configuration to prevent any unauthorized access. It is necessary for Employees to have a set of permissions, while students also need permissions. The purpose of the permission controls is to keep them from accessing all your bank data and documents.

Data Protection and Encryption: An extra layer of security will be provided by encrypting the data; any compromised data will be encrypted, allowing for a good amount of security. Dealing with suspicious activity will also be made easier with the use of powerful antivirus software.

Observation and Record-Keeping: Every bank should have monitoring and logging in place for the safety of its Employees. IDS, which detects and isolates questionable traffic on an ongoing network, is one example of it. In addition to managing connection history, which aids in cyberattacks, logging helps to maintain the threat.

Awareness and Training: Everyone at the banking should understand the significance of network security since improper protection could leaks the confidentiality and integrity of bank data as well as the private information of Customers and shareholders.

Establishing Network Requirements: Determined the goal of the network, which was to create a safe infrastructure that could manage international transactions.

Information Gathering: To identify the best topology for the network, data on various topologies was gathered and analyzed.
Device Selection: To ensure appropriateness and convenience, devices were selected based on how well they met the network's requirements.

Network Security Assurance: To protect the network and guarantee its general safety, security measures were put in place, such as the use of firewalls.

A. Features of the network.

In 2024, a bank network typically employs a hybrid model that blends remote and in-person instruction to maximize learning outcomes. To guarantee smooth connectivity across the university, it makes use of both LAN (local area network) and WAN (wide area network). To have a faster connection, the LAN connection is wired through the network, such as banks, ATM's, lockers and offices. Additionally, a WLAN connection is usually required for the bank employees and managers to have remote access.

In addition to IOT devices like cameras, display boards, TVs for seamless connectivity, the hybrid architecture is made to support a variety of devices. With LAN, the network connection is quicker and more dependable.
Network Setup

The banking services need to be more secure compared to the other platforms. The Cisco ISR (integrated service router) of 7000 and 17.15.1, which controls traffic between the branches, also the router that the ISP uses to deliver internet to the different branches. The Palo Alto Networks Next-Gen Firewalls of versions 11.1 and 7080 series follow for the bare minimum of firewall requirements because the bank service occasionally needs to obtain unauthorized data.

High levels of security and dependability are guaranteed by the multi-layered architecture of the bank network. Network traffic between internal and external systems is managed by the Cisco Catalyst 7080 router YA/YB.10.08.002 which is connected to the internet via an ISP (Internet Service Provider) at the highest level [2]. Using a PAN-OS 11.1 firewall, which offers security barriers, filters traffic, and stops unauthorized access, it is directly connected to its Palo Alto PA-7080. The HPE Aruba Networking 2930U switch, which is positioned beneath the firewall, is connected. It separates the network into VLANs and routes internal traffic, enabling efficient communication between servers, staff, ATMs, and Internet of Things devices. The servers in the following layer are used for bank operations; these include Dell PowerEdge R760 servers, which are set up for functions.

Applications such as mobile and internet banking are supported by the application server.

Data servers are used to store sensitive data, including transaction and customer information. To ensure the integrity of the system, each server runs software like Microsoft SQL Server. [3] These servers also have Jenkins installed to automate continuous integration, and banking applications use Jenkins to guarantee software updates and security. The network is segmented into VLANs beneath the server layer to preserve security and manage traffic.

1. The Internet of Things VLAN is exclusively utilized for surveillance and monitoring devices, such as Honeywell CCTV cameras (Honeywell 20 series IP cameras) [4]

A Cisco Catalyst 7080 wireless controller (version 17.15.1) was utilized for the wireless connection in this infrastructure.

This network also integrates with the cloud, enabling the bank to use AWS or Google Cloud's SaaS solution platform for backups. This architecture reduces vulnerabilities, speeds up operations, and improves security by segmenting networks and integrating with hardware and software. This layer is intended to facilitate continuous banking services delivery and efficient threat response and monitoring. The ATM is used for essential secure connections of the latest model G2500. It helps in providing more flexibility and upgrade options for existing deployments [5]. Also, VLAN of the Employee will be using any laptop devices like dell, Asus with recent windows O.S 24H2.

Below is the detail table of network architecture:

Layers	Model /Device	Function	O.S/ software version	Date
Security Layer	Palo Alto PA-7080 Firewall	Traffic Filtering	11.1	2024
Router	Cisco catalyst 7000 series	Used to maintain the network traffic	17.15.1	2024
Switch	HPE Aruba Networking 2930U	VLANs are different	YA/YB.10.08.0021	
Server	Server Dell PowerEdge R760	Used for managing the database for storage and other tasks	Integration for Microsoft System Centre 7.2.1	2024
Wireless controller	Cisco Catalyst 9800-L Router	Easy wireless access for Managers and employees	17.16.1	2024
IOT VLAN	Honeywell 20 series IP	Surveillance	Firmware v1.2.3	2024

	cameras			
ATM VLAN	G2500 series	ATM transactions are secured	ATM OS Proprietary	2024
VLAN Employee	Dell, Asus	Manager/employee Laptops	O.S 24H2	2024
Access point	Aruba AP- 635 (630 Series)	Gives wireless access to both employees and customers throughout the bank area	Aruba OS 10.4	2024

III. NEWORK DIAGRAM

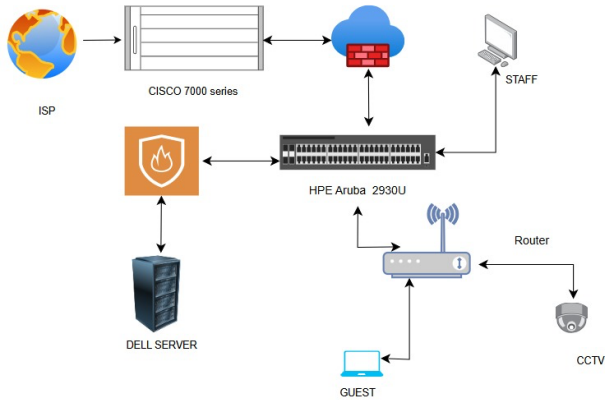

FIGURE 3.1: NETWORK SETUP

IV. ATTACK VECTOR

CVE-2024-42509

Brief description: The Attackers can target devices remotely without needing any physical access but the critical vulnerability in Aruba products will permit the network-based on exploitation. Because the vulnerability allows unauthenticated access, attackers can take advantage of it without having legitimate credentials. Attackers can take advantage of a command injection flaw in the Command Line Interface (CLI) service by sending specially constructed packets to the PAPI (Aruba's Access Point management protocol) over UDP port 8211. A successful exploitation gives attackers privileged access to run any code, which could compromise the operating system that are impacted at serious risk of security breaches.[6]

Post Exploitation: The post-exploitation of the critical vulnerability CVE-2024-42509 affecting HPE Aruba Access. Upon gaining privileged code execution, the attackers can run the specific commands on the compromised system. This can be made to manipulate device configurations and extract sensitive data. This might involve extraction of configuration files and stored credentials for further facilitating unauthorized access to other systems within the network. Attackers might establish a command-and-control channel for further communication with their infrastructure to enable continued exploitation or data theft. The compromised access point may be used to disrupt normal network operations or to carry out a service attack against other devices. These post-exploitation activities could also be a potential activity, which indicates the criticality of the vulnerability and requires timely patching and mitigation strategies.

C2 Activity: CVE-2024-42509 can enable many C2 capabilities, by improving an attacker's position in maintaining control of a compromised system. Once exploited, attackers can establish outbound connections to their C2 infrastructure and issue commands remotely. They may deploy persistent backdoors to ensure prolonged access to the affected devices. Since attackers can continuously manipulate such a compromised device, for their attack persistence, it generally leads to a severe threat that can be posed against the overall security of the network, which may lead to extensive data breaches and serious operational disruptions.[7]

Motive behind Exploitation: The motivations behind the exploitation of CVE-2024-42509 in HPE Aruba Access points are varied and significant, generally driven by the potential to compromise networks and steal data. Through this, an attacker gets privileged access to run arbitrary code on the affected devices, which may result in the compromise of the whole network infrastructure. This makes the vulnerability quite attractive, since it allows attackers to get access to sensitive information. Moreover, attackers may set up long-term backdoors for persistence in system control, enable lateral movement within the network, and widen their influence. [8]

Key Techniques: CVE-2024-42509 attack vectors take advantage of several important techniques that make the possibilities of exploitation more promising. In this case, an attacker can remotely exploit vulnerable Aruba Access Points over the network, as no authentication is required to access the system. The core of the attack involves command injection, attacking a vulnerability in the inner Command Line Interface (CLI) service. Specifically, attackers send specially crafted packets to the PAPI-which is Aruba's Access Point management protocol-UDP port 8211, enabling them to execute arbitrary code with privileged user access on the underlying operating system. This exploitation technique allows for the delivery of custom payloads containing harmful commands or scripts that can be executed on the target system. Successful exploitation, therefore, leads to complete compromise of the vulnerable access points, enabling further malicious activities like data theft, lateral movement within the network, and deployment of additional malware, thus posing a serious threat to network security. [9]

Targeted devices: CVE-2024-42509 mainly consider the following devices:

Aruba Access Points running Instant AOS-8 software versions:

Versions prior to 8.10.0.13

Versions prior to 8.12.0.2

Aruba Access Points running AOS-10 software versions:

Versions prior to 10.4.1.4

Legacy devices running Instant AOS-6.x and Instant AOS-8.x iterations have attained end-of-life (EoL) status. [10]

Vulnerabilities: 9.8(high severity) CVSS Vector:

CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:C/C:L/I:L/A:L [11]

CVE-2024-33513

Brief description: CVE-2024-33513 is an unauthenticated DoS vulnerability in the AP Management service of Aruba ArubaOS that can be exploited through several key attack vectors. Attackers can reach the vulnerability remotely without the need for any authentication. They can crash the normal operation of the affected AP Management service by sending specially crafted packets to the PAPI, which is a protocol used by Aruba for managing Access Points. This vulnerability is present in several versions of ArubaOS, including 10.5.x.x, 10.4.x.x, 8.11.x.x, and 8.10.x.x, which expands the attack surface. If exploited successfully, this will lead to serious service interruptions and network disruptions in affected Aruba devices, thus posing a serious risk to organizational operations and network stability. [12]

Post exploitation: After following the exploitation of CVE-2024-33513, an unauthenticated denial-of-service vulnerability in Aruba ArubaOS, a few serious impacts may be caused to the targeted system. Attackers may use this vulnerability to run arbitrary commands on the affected device and take control over its operations. They can also try to extract sensitive configuration data and stored credentials, which might give them a way to conduct further attacks inside the network. Additionally, they might establish command and control channels for continued communication and control, manipulate system logs to get detection. These possible post-exploitation activities show the CVE-2024-33513 consequently, a need for remediation to protect the integrity and security of a network. [13]

C2 Activity: CVE-2024-33513 is an unauthenticated denial-of-service vulnerability in ArubaOS that does not directly enable C2 activities. The primary impact is against the availability of the AP Management service. However, potential C2-related activities following a successful exploit will involve the Attackers might disrupt normal operations of the affected AP Management service, creating instability in the network, which could be used to perform further attacks. The ability to cause DoS could be used to probe network defenses and identify vulnerable systems. The exploitation of this vulnerability could be a reason to get away with other malicious network activities. [14]

Motive: There could only be one motive to this very particular exploit of CVE-2024-33513 in ArubaOS-to just purely cause a disruption in operational terms. An attacker can make use of this unauthenticated DoS vulnerability to disrupt regular AP Management service and gain network instability. The vulnerability could also be exploited for reconnaissance purposes, allowing the attackers to probe network defenses and identify vulnerable systems. Additionally, it might be used as a distraction technique, removing the resources from other malicious activities occurring on the network. While CVE-2024-33513 does not directly enable data theft or system compromise, the capability for service disruption simply makes it one of the biggest threats against network availability.[15]

Key techniques: CVE-2024-33513 is an unauthenticated denial-of-service vulnerability in ArubaOS that can be exploited through several key techniques. Attacks may be performed over the network, remotely against the AP Management service. The exploitation involves sending specially crafted packets to the PAPI - Aruba's Access Point management protocol - to trigger the vulnerability. Successful exploitation results in service disruption, which would be the normal operation of the affected AP Management service. Continuous exploitation may lead to resource exhaustion, potentially causing system instability or crashes. The specific attack targets vulnerable versions of ArubaOS: 10.5.x.x, 10.4.x.x, 8.11.x.x, and 8.10.x.x. These techniques together enable attackers to effectively exploit CVE-2024-33513 and may cause significant disruption to network operations and availability in affected systems.[15]

Vulnerability: The severity of this vulnerability is high, with a CVSS score 9.8 out of 10

CVE-2024-2550

Brief description: CVE-2024-2550 is a different vulnerability in the Global Protect gateway of Palo Alto Networks PAN-OS that could let an unauthenticated attacker DoS the device. To attack, one would just need to send specially constructed packets to the Global Protect service to crash it, and multiple exploitation attempts of this vulnerability will lead to the firewall to go into a maintenance mode and disrupt all network operations. The vulnerability has a low attack complexity and requires no authentication, making it somewhat easy for attackers to leak data, thus pointing to the potential impact of the vulnerability on the affected systems, especially those in environments that rely on firewalls from Palo Alto Networks for security. [16][17].

C2 Activity: CVE-2024-2550 does not provide an avenue for C2 because it disrupts service as opposed to providing unauthorized access or code execution. However, using the resulting downtime or a maintenance mode of the firewall, attackers could facilitate secondary activities. For example, the attackers may use other vulnerabilities or weaknesses in the network during a disruption to establish C2 channels. These might use encrypted protocols such as TLS/SSL or SSH to have persistence with compromised systems. Service disruption may also act as a diversion to conduct payload deployment or reconnaissance activities by adversaries without being noticed. While CVE-2024-2550 itself does not directly lead to C2 activity, its exploitation may provide opportunities for broader malicious campaigns. [18]

Motive: The motives for the exploitation of CVE-2024-2550 is attackers may seek to leverage this vulnerability to initiate a denial-of-service condition that stops the Global Protect service on the firewall. These could have significant operational impacts, including downtime for critical services and disruption of secure remote access for users. Furthermore, because an attacker can repeatedly exploit this vulnerability, they might force the firewall into maintenance mode and make manual recovery more complex. This will involve actions aimed at several malicious objectives: testing an

organization's security infrastructure, distracting IT staff in support of executing other attacks, or for the sheer demonstration of capabilities that cause disruptions. [18]

Key techniques: The attack can be initiated remotely by an attacker by sending specially crafted packets to the global Protect service, which will trigger a DoS condition. This vulnerability is particularly concerning because it allows unauthenticated access, meaning attackers do not need credentials to exploit it. By leveraging packet crafting techniques, attackers can leverage the null pointer dereference vulnerability to crash the global Protect service. Repeated exploitation of the vulnerability can force the firewall into maintenance mode, further disrupting network operations. With low attack complexity, this vulnerability is within reach of even unsophisticated attackers, making it a serious threat to organizations that rely on Palo Alto Networks firewalls for secure remote access and protection of their networks. These techniques underline the need to apply patches and implement robust monitoring to mitigate potential exploitation.

Vulnerability: The severity of this vulnerability is high, with a CVSS score of 8.7.

V. MITIGATIONS

CVE-2024-42509 Mitigations (Aruba Access Points)

1. Immediate Patching:

Upgrade Firmware: Update affected Aruba Access Points to the latest firmware versions:[6]

AOS-8: 8.10.0.13 or later, 8.12.0.2 or later

AOS-10: 10.4.1.4 or later

Legacy Devices: Updates of any legacy devices running Instant AOS-6.x and Instant AOS-8.x must also be made.

2. Network Segmentation:

Isolate Vulnerable Devices: Utilize network segmentation to reduce the number of systems that have access to the vulnerable device and to limit the attack surface.

3. Access Control:

Limit Unauthenticated Access: Implement access controls to limit unauthenticated access to the management interfaces of Aruba devices.

4. Monitoring and Logging:

Improve Monitoring: Utilize extensive monitoring solutions to detect suspicious activities or unauthorized access attempts.

Log Analysis: Perform periodic log analysis for signs of exploitation attempts or suspicious behavior.

Mitigations for CVE-2024-33513 (ArubaOS) [12]

1. Firmware Updates:

Apply Patches to Vulnerable Versions: Update ArubaOS to versions that address the DoS vulnerability:

AOS 10.5.x.x, 10.4.x.x, 8.11.x.x and 8.10.x.x updates should be done with the latest stable releases.

2. Rate Limiting:

Rate Limiting Implementation: This can be used to prevent the possibility of a DoS attack against management services by rate-limiting the number of processed requests.

3. IDS:

IDS Solutions Deployment: IDS can be used for monitoring traffic pattern(s) and/or identifying possible attempts to exploit AP Management service vulnerabilities.

4. Incident Response Plan:

Establish a response plan that outlines steps to be taken in case of service disruption due to DoS attacks.

CVE-2024-2550 Mitigations (Palo Alto Networks)[18]

1. Update GlobalProtect Gateway:

Apply Security Patches: The GlobalProtect gateway should be updated to those versions which have fixed the null pointer dereference vulnerability.

2. Service Monitoring:

Continuous Monitoring: Firewalls services should be continuously monitored against any kind of unusual patterns that could indicate exploitation attempts.

3. Redundancy and Failover:

Establish Redundant Systems: Establish redundancy or failover mechanisms that can help keep the network available in case of disruptions due to exploitation. 4. User Education: Train Staff on Security Practices: Impart training sessions to the staff for identifications and response against the potential security threats related to network operations.

V. CONCLUSION

This report is based on the network to be built within a financial institution with the aim of finding and solving any security risks. In this regard, we aimed at understanding how the organization's servers, routers, and firewalls work together, and then went further to select the best that keeps everything secure. A network was built with dissimilar devices and configurations, which should stand for future challenges and grow with the growth of the organization.

During the research study, a few major security issues were identified, such as command injection and DoS attacks. Command injection is the process of injecting malicious code into normal systems, which can lead to stolen or compromised data. DoS attacks block access to the network, often asking for a ransom to restore access. These risks just show how important it is to have strong security measures that protect both the organization's data and daily operations.

Another important finding of the research is that updating the software is crucial. Testing for vulnerabilities, coupled with the timely installation of updates, helps in keeping the systems updated. Using outdated software might seem an easy way of saving finances, but it opens a network to several critical threats. Even with limited resources, it's crystal clear that one of the ways to keep the network safe and running smoothly is by updating everything.

VI. REFERENCES

[1]https://live.paloaltonetworks.com/t5/user/viewprofilepage/user-id/214353, “Empowering and Securing Banking and Financial Organizations,” *live.paloaltonetworks.com*, Jun. 09, 2023. https://live.paloaltonetworks.com/t5/general-articles/empowering-and-securing-banking-and-financial-organizations/ta-p/545427

[2]“HPE Aruba Networking 2930F Switch Series,” *PSNow*, 2024. https://www.hpe.com/psnow/doc/a00137057ENW (accessed Dec. 12, 2024).

[3]“PowerEdge R760 Rack Server,” *Dell*. https://www.dell.com/en-ie/shop/ipovw/poweredge-r760 (accessed Dec. 10, 2024).

[4]“30 Series IP Camera | Surveillance Cameras | Cameras | Video Systems | Surveillance Cameras | Honeywell Building Solutions,” *Honeywell.com*, 2024. https://buildings.honeywell.com/us/en/products/by-category/video-systems/cameras/fisheye-cameras/30-series-ip-camera (accessed Dec. 17, 2024).

[5]“Genmega - G2500,” *ATM Brokerage*, Feb. 14, 2024. https://atmbrokerage.com/product/genmega-g2500/ (accessed Dec. 14, 2024).
[6]daksh sharma, “Critical Command Injection Vulnerabilities in HPE Aruba APs,” *Cyble*, Nov. 12, 2024. https://cyble.com/blog/hpe-aruba-access-points-have-critical-command-injection-vulnerabilities/ (accessed Dec. 16, 2024).
[7]A. Potter, “Post Exploitation Activities on Fortinet Devices: A Network-Based Analysis,” *Darktrace.com*, Oct. 30, 2024. https://darktrace.com/blog/post-exploitation-activities-on-fortinet-devices-a-network-based-analysis
[8]“CVE-2024-42509 - Securin,” *Securin* -, Nov. 10, 2024. https://www.securin.io/vulnerability-notice/cve-2024-42509/
[9]RecordedFuture, “CVE-2024-42509 Description, Impact and Technical Details,” *Recordedfuture.com*, 2024. https://www.recordedfuture.com/vulnerability-database/CVE-2024-42509
[10]Ionut Arghire, “HPE Patches Critical Vulnerabilities in Aruba Access Points,” *SecurityWeek*, Nov. 08, 2024. https://www.securityweek.com/hpe-patches-critical-vulnerabilities-in-aruba-access-points/
[11]“Understanding the CVSS Base Score :: Black Duck Continuous Dynamic Documentation,” *Whitehatsec.com*, 2024. https://source.whitehatsec.com/help/sentinel/secops/cvssv3-factors.html (accessed Dec. 22, 2024).
[12]“CVE-2024-33513: Addressing Unauthenticated Denial-of-Service Vulnerability in ArubaOS,” *Ogma.in*, 2024. https://ogma.in/cve-2024-33513-addressing-unauthenticated-denial-of-service-vulnerability-in-arubaos
[13]A. Potter, “Post-Exploitation Activities on PAN-OS Devices: A Network-Based Analysis,” *Darktrace.com*, Jun. 20, 2024. https://darktrace.com/blog/post-exploitation-activities-on-pan-os-devices-a-network-based-analysis (accessed Dec. 22, 2024).
[14]“CVE-2024-33513,” *Debian.org*, 2024. https://security-tracker.debian.org/tracker/CVE-2024-33513 (accessed Dec. 22, 2024).
[15]“CVE-2024-30368, CVE-2024-30369 – A10 ACOS Command Injection Remote Code Execution and Privilege Escalation - A10 Support,” *A10 Support*, Sep. 16, 2024. https://support.a10networks.com/support/security_advisory/cve-2024-30368-cve-2024-30369-a10-acos-command-injection-remote-code-execution-privilege-escalation/ (accessed Dec. 22, 2024).
[16]“CVE-2024-2550,” *Feedly.com*, 2024. https://feedly.com/cve/CVE-2024-2550 (accessed Dec. 22, 2024).
[17]“Working with PaloAlto to identify CVE-2024-2550,” *Ac3.com.au*, 2024. https://www.ac3.com.au/resources/discovery-of-CVE-2024-2550/ (accessed Dec. 22, 2024).
[18]Yair Divinsky, “Closing 2024 trending CVES and exploits - Last month’s trending CVEs to watch out from,” *Vulcan Cyber*, Dec. 11, 2024. https://vulcan.io/blog/blog/november-trending-cves/ (accessed Dec. 22, 2024).
[19]“Comprehensive Analysis of CVE-2024-2550: Mitigating Denial of Service in PAN-OS GlobalProtect Gateway,” *Ogma.in*, 2024. https://ftp.ogma.in/comprehensive-analysis-of-cve-2024-2550-mitigating-denial-of-service-in-pan-os-globalprotect-gateway (accessed Dec. 22, 2024).