

**Penetration Testing Report (DELTA)**

**Date:** 10 June 2024 – 14 June 2024

**Testers:** Zachary Skweres, Juan Angustia, Keavon Fininen

**Executive Summary:**

During the penetration test conducted from 10 June 2024 to 14 June 2024, critical vulnerabilities were discovered within the target system. These vulnerabilities pose significant risks to the security and integrity of the system and require immediate attention. The most critical findings include an exploit within the directory accessed via "http://192.168.122.47/console," leading to the discovery of a compromised admin portal with broken credentials. Additionally, remote code execution (RCE) vulnerabilities were identified, allowing attackers to execute arbitrary commands with www-data privileges. The exploitation of directory traversal, default credentials on the PFSense router, and vulnerabilities in command execution further exacerbate the risk. This report provides detailed findings, recommendations, and remediation steps to enhance the system's security posture.

**Penetration Testing Glossary:**

1. **Findings……………………………………………. (Page 3)**
2. **Exploit within Directory…….……………………**  (Page 4)
3. **Compromised Admin Portal…….……………….**  (Page 5)
4. **Remote Code Execution (RCE)……..……………**  (Page 6)
5. **Default Credentials on PFSense Router…**…..…… (Page 7)
6. **Vulnerability in Command Execution……..……..**  (Page 8)
7. **Listener on Open Port.**.…………….…………….... (Page 9)
8. **Network Enumeration…….……………………….**  (Page 10)
9. **Vulnerability in Port 10000:** ……………………… (Page 11)
10. **Socks Proxy Usage……………………………** (Page 12)
11. **Recommendations & Conclusion…………… (Page 13)**

**Findings:**

| **Finding** | **Category** | **Gaining Access** | **Information Disclosure** | **Initial Exploitation** | **Privilege Escalation** |
| --- | --- | --- | --- | --- | --- |
| Exploit within Directory | Critical | Yes | No | Yes | No |
| Compromised Admin Portal | Critical | No | Yes | No | No |
| Remote Code Execution (RCE) | Critical | Yes | No | Yes | No |
| Default Credentials on PFSense Router | High | Yes | No | No | No |
| Vulnerability in Command Execution | High | Yes | No | Yes | No |
| Listener on Open Port | High | Yes | No | Yes | No |
| Network Enumeration | Medium | No | No | No | Yes |
| Vulnerability in Port 10000 | High | Yes | No | No | No |
| Socks Proxy Usage | Medium | Yes | No | No | No |

***Exploit within Directory (CRITICAL)***

*Components:*

All Affected components

*Status:*

Resolved/ Unresolved

*Description:*

This finding denotes the discovery of an exploit within a specific directory, potentially enabling unauthorized access or manipulation of critical system resources.

*Impact:*

 **Unauthorized Access:** Attackers may gain entry into sensitive directories, potentially compromising the confidentiality and integrity of data.

 **Information Disclosure:** Sensitive information stored within the compromised directory could be exposed, including user credentials, configuration files, or proprietary data.

 **Financial Loss:** Remediation efforts, legal fees, and loss of business due to reputational damage can result in significant financial losses for the organization.

*Technical fix:*

A technical fix for an exploit within a directory involves applying patches, configuring access controls, and deploying monitoring tools to prevent unauthorized access or manipulation of files. By implementing these measures, organizations can mitigate the risk of exploitation and enhance the security of their systems.

*Remediation:*

Updating configurations and implementing access controls to prevent unauthorized access or manipulation. Regular security assessments can help identify and address vulnerabilities proactively.

*Technical Details:*

These details provide crucial insights to security professionals and system administrators, enabling them to comprehensively address the risk posed by the exploitation and safeguard the integrity of the system.

***Compromised Admin Portal (CRITICAL)***

*Components:*

Affects the administrative interface, user accounts, configuration settings, and potentially connected systems, leading to security risks and potential unauthorized access to sensitive data or resources. It may also compromise the integrity of associated services and undermine overall system security.

*Status:*

Resolved/ Unresolved

*Description:*

Unauthorized access or manipulation of an administrative interface, potentially leading to the compromise of user accounts, configuration settings, and system integrity.

*Impact:*

Potentially leads to data breaches or system manipulation.

*Technical fix:*

Immediately revoking compromised credentials, conducting a thorough security audit to identify vulnerabilities, and implementing stronger authentication measures and access controls to prevent unauthorized access in the future.

*Remediation:*

Thoroughly investigate the breach to identify vulnerabilities and implement robust authentication protocols and access controls to prevent future unauthorized access.

*Technical Details:*

Identifying the specific vulnerabilities or weaknesses exploited, understanding the attack vectors used by the attackers to gain unauthorized access, and analyzing the impact of the compromise on system integrity and data confidentiality.

***Remote Code Execution (RCE) (CRITICAL)***

*Components:*

Affects web applications, servers, or network devices, allowing attackers to execute arbitrary code remotely.

*Status:*

Resolved/ Unresolved

*Description:*

Refers to a security vulnerability that enables attackers to execute arbitrary code on a target system remotely, often leading to unauthorized access, data manipulation, or system compromise. Exploitation of RCE vulnerabilities can have severe consequences, including data breaches, service disruptions, and potential takeover of the affected system by malicious actors.

*Impact:*

Allow attackers to execute arbitrary commands on a target system remotely, leading to unauthorized access, data exfiltration, and complete system compromise. The exploitation of RCE vulnerabilities poses significant security risks, potentially resulting in financial loss, reputational damage, and legal consequences for affected organizations.

*Technical fix:*

Applying patches or updates to affected software, implementing strict input validation mechanisms, and deploying intrusion detection systems to detect and block malicious code execution attempts.

*Remediation:*

Promptly applying patches or updates to affected software, disabling unnecessary services or functionalities, and implementing strong access controls and network segmentation to limit the attack surface.

*Technical Details:*

Occurs when attackers exploit vulnerabilities in a system to execute arbitrary code remotely, potentially leading to unauthorized access, data theft, or system compromise.

***Default Credentials on PFSense Router (HIGH)***

*Components:*

Administrative interface and underlying network configuration settings, potentially enabling unauthorized access to sensitive network resources.

*Status:*

Resolved/ Unresolved

*Description:*

Usernames and passwords that are commonly set by manufacturers or administrators. These credentials, if unchanged, pose a security risk as they can be easily exploited by attackers to gain unauthorized access to the router's administrative interface and potentially compromise the entire network.

*Impact:*

Can lead to unauthorized access to the router's administrative interface, enabling attackers to modify network configurations, intercept traffic, or launch further attacks within the network.

*Technical fix:*

Involves changing the default usernames and passwords to strong, unique credentials immediately after deployment, ensuring that access to the administrative interface is restricted to authorized personnel only.

*Remediation:*

Enforcing strict access controls and implementing network segmentation can help prevent unauthorized access and mitigate the risk of further exploitation within the network.

*Technical Details:*

Presence of pre-configured usernames and passwords, often provided by the manufacturer or administrator for initial setup.

***Vulnerability in Command Execution (HIGH)***

*Components:*

Typically include the software or system where the vulnerability exists, as well as any associated functionalities or services that can be exploited to execute arbitrary commands.

*Status:*

Resolved/ Unresolved

*Description:*

Refers to a security flaw that allows attackers to execute arbitrary commands on a target system. Exploitation of this vulnerability can lead to unauthorized access, data manipulation, or complete compromise of the affected system, posing significant risks to its integrity and confidentiality.

*Impact:*

Enabling attackers to execute arbitrary commands on a target system, potentially leading to unauthorized access, data exfiltration, or system compromise.

*Technical fix:*

Implementing input validation mechanisms to sanitize user inputs, restricting command execution to authorized users and limiting their privileges. Additionally, applying security patches, updates, and configuring firewalls or intrusion detection systems can help mitigate the risk of exploitation and enhance overall system security.

*Remediation:*

Conducting regular security audits and employee training on secure coding practices can help prevent future occurrences and enhance overall system security.

*Technical Details:*

Involve identifying the specific flaw in the software or system that allows attackers to inject and execute arbitrary commands. Exploitation typically occurs through insufficient input validation or improper handling of user-supplied data, enabling attackers to bypass security mechanisms and execute commands with elevated privileges, posing significant risks to system integrity and data confidentiality.

***Listener on Open Port (HIGH)***

*Components:*

Network service or application running on the open port, as well as any associated functionalities or services that interact with it.

*Status:*

Resolved/ Unresolved

*Description:*

Network service or application actively waiting for incoming connections on a specific port, facilitating communication between clients and servers. It acts as a gateway for data transmission, monitoring designated ports for incoming traffic and enabling the exchange of information between networked devices.

*Impact:*

Potential entry point for attackers to gain unauthorized access to a system or network.

*Technical fix:*

Configuring firewalls to restrict access to only necessary ports and implementing intrusion detection systems to monitor for suspicious activity.

*Remediation:*

Regular port scanning and vulnerability assessments can help identify and address any vulnerabilities in open ports, ensuring a more secure network environment

*Technical Details:*

Involve configuring a network service or application to bind to a specific port and listen for incoming connections from clients.

***Network Enumeration (Medium)***

*Components:*

Network infrastructure and security mechanisms, such as firewalls and intrusion detection systems, may also be impacted, depending on the methods and extent of the enumeration activity.

*Status:*

Resolved/ Unresolved

*Description:*

Gathering information about network devices, services, and resources, such as IP addresses, open ports, and active hosts, to create a comprehensive map of the network topology and identify potential attack vectors.

*Impact:*

Provides attackers with valuable information about the network's infrastructure, potential entry points, and security weaknesses.

*Technical fix:*

Implementing security measures such as network segmentation, firewalls, and intrusion detection systems to limit unauthorized access and detect scanning activities.

*Remediation:*

Regular network monitoring and vulnerability assessments can help identify and address potential weaknesses, ensuring a more resilient and secure network infrastructure.

*Technical Details:*

Scanning the network for active hosts, services, and open ports using tools such as Nmap or masscan. This reconnaissance technique involves sending packets to target devices and analyzing their responses to gather information about the network topology, potentially exposing vulnerabilities and aiding in the planning of cyberattacks.

***Vulnerability in Port 10000 (HIGH)***

*Components:*

Typically include the network service or application running on port 10000 and any interconnected systems or services that rely on it for functionality.

*Status:*

Resolved/ Unresolved

*Description:*

Security flaws present in a network service or application running on port 10000, potentially allowing unauthorized access or exploitation by attackers.

*Impact:*

Exploitation of this vulnerability can lead to unauthorized data access, service disruptions, and potential compromise of sensitive information, necessitating immediate remediation efforts to mitigate potential risks and secure the affected port.

*Technical fix:*

Applying security patches or updates to the affected service or application running on the port and implementing access controls or firewall rules to restrict unauthorized access.

*Remediation:*

Regular vulnerability scanning and proactive monitoring can help identify and address potential weaknesses, ensuring a more secure network environment.

*Technical Details:*

The technical details of a Vulnerability in Port 10000 involve identifying the specific security flaw present in the network service or application running on port 10000, such as a buffer overflow or authentication bypass vulnerability. Exploitation typically occurs by sending specially crafted packets to the port, allowing attackers to gain unauthorized access, execute arbitrary code, or disrupt service functionality, highlighting the importance of promptly applying patches and implementing appropriate security measures.

***Socks Proxy Usage (MEDIUM)***

*Components:*

Proxy server itself, client applications utilizing the proxy for network communication, and the network infrastructure facilitating proxy connections.

*Status:*

Resolved/ Unresolved

*Description:*

Redirecting network traffic through a proxy server, providing anonymity and bypassing network restrictions for client applications.

*Impact:*

Enables users to bypass network restrictions and conceal their online activities, potentially facilitating illicit activities such as unauthorized access, data exfiltration, or malware distribution.

*Technical fix:*

Implementing network filtering mechanisms to block unauthorized proxy connections and monitoring network traffic for signs of proxy usage.

*Remediation:*

Enforcing strict access controls and educating users about the risks associated with proxy usage can help mitigate the use of Socks proxies for malicious purposes and enhance overall network security.

*Technical Details:*

Involve configuring client applications to communicate with a proxy server, which then forwards network requests on behalf of the client. This process typically involves establishing a connection to the proxy server, authenticating the client, routing traffic through the proxy, providing anonymity and bypassing network restrictions for the client application.

***Recommendations:***

1. Immediately address the identified vulnerabilities, starting with the patching of the exploited directories and services.
2. Implement proper access controls and authentication mechanisms to prevent unauthorized access to sensitive functions and data.
3. Change default credentials on the PFSense router and other network devices to mitigate the risk of unauthorized access.
4. Conduct thorough security assessments regularly to identify and remediate emerging vulnerabilities promptly.
5. Educate system administrators and users on best practices for securing systems and data, including password hygiene and system hardening techniques.

***Conclusion:***

The penetration test revealed critical vulnerabilities within the target system, posing significant risks to its security and integrity. Urgent remediation is required to mitigate these vulnerabilities and enhance the system's security posture. The recommendations provided in this report should be promptly implemented to safeguard against potential exploitation and data breaches. Regular security assessments and proactive measures are essential to maintain a robust and resilient security posture against evolving threats.