|  |  |  |
| --- | --- | --- |
| **NOC REPORTING TEMPLATE** | | |
| Date Updated: C5/27/2023 | Name: Damian J. Yates | |
| ***A. Introduction*** | | |
| In the wake of heightened reports of web exploits targeting adjacent businesses, a board meeting at Psinuvia, Inc. was convened, during which pressing security issues were discussed. Responding to these increasing external threats, Psinuvia, Inc. engaged the expertise of Autojor Security Consultants to undertake a rigorous security audit. This extensive examination aimed to evaluate the company's existing cybersecurity practices as well as determining improvements to its broader business processes and procedures.  Autojor recently provided a comprehensive report that encapsulates their exhaustive appraisal of the company's security stance. This document distils the key findings of the report, offering an overview of Psinuvia, Inc.'s security landscape. It spotlights areas necessitating augmentation and recommends potential strategies to rectify the identified weaknesses in the company's security framework. | | |
| ***B. Scan Summary*** | | |
| Attached are several reports generated by Autojor using AlienVault and NMAP on 09/13/2021. The Vulnerability Assessment report provided data points between 07-01-2019 to 01-25-2020 from Alien Vault OSSIM and detected and logged 131 vulnerabilities identified across 3 systems. Psinuvia IT Operations staff has reviewed the data found in the report and confirmed the vulnerabilities found by the assessment.  Out of the reported vulnerabilities, 35% are categorized as "Informational" data points, which pose little to no threat to the organization. Host-172-20-1-131 presenting the most alarming vulnerabilities, four of which are deemed serious. Foremost among these is an unattended security update which could potentially expose the system to remote attackers. These attackers may exploit port 445 (SMB) to execute code on the target server, leading to potential data exfiltration.  The remaining three serious vulnerabilities stem from software that has outlived its support lifecycle, specifically PHP (Ports 443 and 80) and OpenSSL (Port 443). As these software versions have reached end-of-life, they cease to receive crucial security updates from the vendor, which leaves the host susceptible to latent, unfixed security threats.  To further validate the findings of the AlienVault assessment and gather additional information from the servers, Autojor employed NMAP, a network scanning tool.  The attached AlienVault Alarms Report offers a comprehensive overview of security events and incidents detected by the AlienVault security appliance. This report provides valuable insights into potential threats, detected attacks, and suspicious activities across the organization's network, systems, and perimeter. By referring to this report, security analysts can effectively leverage server, network, and firewall logs to correlate aggregated data points, documenting the source, target, and timing of potential assaults.  A brief synopsis of the vulnerabilities found in Psinuvia, Inc.'s systems consists of the following:  1. End of Life Software Detected: Outdated software that is no longer supported, posing a security risk.  2. Missing Security Updates: Failure to apply necessary security patches and updates, leaving systems vulnerable to known exploits.  3. Software with Unpatched Vulnerabilities: Existing software containing known vulnerabilities that have not been addressed through patches or updates.  4. Expired SSL Certificates: SSL certificates used for secure communication have expired, potentially exposing sensitive data to unauthorized access.  5. Untrusted Certificate Authorities: The presence of certificate authorities that are not trusted, undermines the integrity and authenticity of SSL/TLS connections.  6. Misconfigured SMTP Server: Configuration issues with the Simple Mail Transfer Protocol (SMTP) server, potentially allowing unauthorized access or abuse.  7. Open/Unfiltered TCP/UDP Ports: TCP/UDP ports that are accessible without appropriate security measures, increase the risk of unauthorized access or attacks.  The attached NMAP Scan report provides a comprehensive report of the unfiltered ports which includes service and OS versions.  8. Misconfigured Web Server: Inappropriate configuration of the web server, potentially leading to security vulnerabilities or unauthorized access.  9. Version of PHP Has a Vulnerability: The PHP programming language version in use contains known vulnerabilities that can be exploited by attackers.  10. PHPINFO File Publicly Accessible: The phpinfo file, which provides detailed information about the PHP environment, is accessible to the public, potentially exposing sensitive information.  11. SSL/TLS Using Weak Algorithms: Weak encryption algorithms are employed in SSL/TLS protocols, making secure communication susceptible to attacks.  12. IMAP Misconfiguration: The Internet Message Access Protocol (IMAP) server is misconfigured, potentially leading to security weaknesses or unauthorized access.  These vulnerabilities highlight specific areas of concern within Psinuvia, Inc.'s security posture that requires immediate attention and remediation to ensure the protection of their systems and data. To address these vulnerabilities at an initial stage, firewall rules were implemented to block traffic originating from the identified sources and targeting the vulnerable systems. In addition, change control requests have been created and submitted for approval to address the missing updates and apply necessary application upgrades. To enhance the security of passwords and mitigate the risk posed by clear text vulnerabilities, a change request has been generated to implement password salting across all systems.  While there is currently no immediate evidence of data exfiltration or criminal activity at Psinuvia, Inc., it is essential to note that RSA-encrypted data at rest and in transit contain sensitive information governed by HIPAA and PCI compliance regulations. Therefore, proper classification and protection measures must be in place. As a result, Psinuvia, Inc. is actively conducting a comprehensive investigation to determine the extent, if any, of the compromise and ensure the security of the highly valuable sensitive data.  **Basic Assessment Questions:**  • Is the information confirmed to be correct and accurate? The information has been verified for accuracy through scans conducted by Psinuvia's IT security team. The incident response team has validated the dates of the attacks against the provided reports.  • Who, what, when, where, why, and how? On 1/24/2020 at 10:25 PM, the alarms report indicated that Host172.20.1.131 and Host-172-20-1-129 were targeted by AlienVault and 10.216.31.246 between the dates of 7/1/2019 and 01/25/2020. The attacks involved various methods such as SQL injection, multiple SQL injections from the same source IP, cross-site scripting, and brute force authentication through SSH. At present, the intentions of the attacker remain unknown.  • What information is available from the firewall, router, server, system, intrusion detection system (IDS), system logs, etc.? Psinuvia’s IT security team has access to information regarding the origin of the attacks, including the host details, as well as the specific types of attacks. By correlating this information, the security team can receive real-time updates to stay vigilant against future attacks.  • What type of data is involved, and what is its classification? Fortunately, no data loss has been reported. However, it is important to note that Psinuvia, Inc stores private healthcare information (PHI), which is classified as sensitive.  • Are there obscenities, child pornography, or confrontational data? Based on the information received, there is no such data present in our systems currently.  • Is there criminal activity? An ongoing investigation is being conducted to determine if any criminal activity took place during the attacks.  • Is the data protected by an encryption solution? Psinuvia IT security team employs RSA encryption to safeguard customer and corporate data at rest and in transit.  • What is the magnitude of the systems being impacted? Currently only the web servers have been impacted by the attacks. However, we are actively implementing measures to detect and deter future attacks across the entire Psinuvia Network and Server Infrastructure.  • Is the event still in progress? No, the security event is no longer in progress.  • Has preliminary containment been performed? Yes, the security team have taken steps to deny all traffic originating from the attacking hosts. Additionally, to mitigate brute force attacks, salting of saved passwords has been implemented.  • What is the estimated value of the impacted data and systems? If a successful attack were to occur, the PHI would be of invaluable importance, and Psinuvia, Inc. could potentially face fines from HIPAA, GPDR, PCI regulations due to data loss. Currently, we are conducting an asset valuation of our systems to determine their value. | | |
| ***C. Detailed Analysis*** | | |
| Upon identifying the network vulnerabilities in the conducted scans, penetration testing or 'pen testing' can be initiated to assess the exploitability of these weaknesses. This ethical hacking exercise will enable Psinuvia and its IT department to gauge the potential depth of an attacker's network penetration and identify which systems or data might be compromised.  The subsequent course of action will hinge on the findings of this penetration test and the risk assessment derived from it. These results will establish a foundational measure of the additional security measures required to bolster the network, identify any data that could have been breached, and pave the way for policy updates and modifications to the incident response plan. | | |
| ***D. Scan Response*** | | |
| Psinuvia, Inc. has classified this incident with a high severity rating due to an unusually elevated level of intruder scanning and probing activities. In response to this, the Incident Response Protocol was initiated which preemptively addressed the incident within an expedited timeframe of 4 hours. Key personnel, including the CISO, CTO, Legal Department, and the Director of Security Operations, were engaged and received briefings which provided them with updates every two hours until the threat was isolated, ensuring the continuity of Psinuvia’s operations.  The Incident Response team worked diligently to identify and mitigate all potential vulnerabilities, reinforcing the security of Psinuvia’s systems. During this process, open communication with the escalation group was maintained, offering them comprehensive weekly updates in a dedicated meeting, until all necessary security measures were implemented and verified.  As of now, there are no indications of a data breach. However, Psinuvia, Inc. will work to identify the source of the breach in future investigations. Upon the conclusion of the investigation, Psinuvia will collaborate with the corporate Legal and Regulatory department to ascertain the appropriate legal and regulatory notification procedures per relevant laws and regulations. | | |
| ***E. Remediation*** | | |
| Psinuvia, Inc. response to the incident follows the protocols outlined in NIST 800-61 Chapter 3, which provides a robust framework for effectively quarantining and remediating cyber (National Institute of Standards and Technology, 2012). As part of the incident team’s containment strategy, they plan to redirect the attacker to a honeypot, an isolated controlled sandbox environment. This will allow security analysts to safely monitor the attacker's activities and gather crucial evidence, providing insights into their intentions without risking additional damage or disruption to Psinuvia’s operations.  Following NIST guidelines, a strategic remediation procedure will commence while the attack is contained. This includes methodical steps to ensure the remediation of the incident components to thwart further attacks ( (National Institute of Standards and Technology, 2012). Given the brute force authentication's success, our immediate action will be to disable all compromised accounts.  Specific vulnerabilities identified on Host-172-20-1-131 will be addressed in line with recommended solutions, prioritizing critical vulnerabilities. As an urgent measure, the incident response team has procured updated versions of OpenSSL and PHP to be installed, complemented by the latest security patches.  Further, the Security team will be intensifying defensive measures by augmenting system logging and network monitoring capabilities (National Institute of Standards and Technology, 2012), to ensure early detection and prevention of future attacks. | | |
| ***F. Recommendations*** | | |
| Administrative Controls:   1. To bolster Psinuvia’s defenses against brute force attacks, the security team will revise password management policies. This change will necessitate the creation of passwords that are at least 16 characters long and incorporate a mix of uppercase and lowercase letters, special characters, and numbers. Such complexity and length will extend the time required for a brute-force attack to succeed, making such attacks infeasible (National Institute of Standards and Technology, 2020). 2. A proactive stance is essential for cybersecurity. As such, Psinuvia, Inc. will establish a policy requiring our Cybersecurity IT team to execute vulnerability scans monthly. Any identified critical and high vulnerabilities will be addressed within a strict 48-hour timeframe from detection, as prescribed by the NIST's guide to vulnerability management (National Institute of Standards and Technology, 2011). 3. Furthermore, an emphasis on the importance of training and education for maintaining cybersecurity is recommended. The introduction of a comprehensive training program, including incident response simulations should be adopted. Such exercises will enhance Psinuvia and its employees’ ability to react effectively and efficiently to real-world cyber threats and incidents. | | Technical Controls:   1. To strengthen resilience against brute force attacks, the practice of “defense in depth” will be adopted. First, salting of all hashed passwords will be performed. This practice introduces an additional layer of complexity to hashed stored passwords, making them significantly harder to crack (National Institute of Standards and Technology, 2020). In conjunction with this practice, Psinuvia’s IT Team will enable an account lockout policy that is triggered after three unsuccessful login attempts within a 30-minute window, thereby further deterring brute force attacks (Scarfone & Souppaya, 2009). 2. Psinuvia’s network infrastructure will also be augmented by situating all external internet-facing assets in an isolated subnet secured with a Next-Gen Firewall. This defensive measure ensures that, in the event of future intrusions, the impact will be isolated, limiting any potential harm (Cisco Systems, 2007). 3. To obscure internal infrastructure details from potential attackers, Psinuvia’s Network Engineering Team will work with Network Administrators to configure Network Address Translation (NAT) for all devices accessible via the public internet. By concealing internal IP addresses, it will be considerably more challenging for attackers to exploit internal systems (Cisco Systems, 2009). |

# References

Cichonski, P., Millar, T., Grance, T., & Scarfone, K. (2012). *Computer Security Incident Handling Guide.* Retrieved from NIST Special Publication: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf

Cisco Systems. (2007). *SAFE: A security blueprint for enterprise networks*. Retrieved from Cisco Systems: https://www.cisco.com/c/en/us/about/security-center/network-security.html

Cisco Systems. (2009). *Understanding Network Address Translation.* Retrieved from Cisco Systems: https://www.cisco.com/c/en/us/support/docs/ip/network-address-translation-nat/26704-nat-faq-00.html

National Institute of Standards and Technology. (2011). NIST Special Publication 800-39.

National Institute of Standards and Technology. (2012). NIST Special Publication 800-61. Retrieved from Computer Security Incident Handling Guide.: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf

National Institute of Standards and Technology. (2020). NIST Special Publication 800-63B. Retrieved from Digital Identity Guidelines: Password Use.: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-63b.pdf

Scarfone, K., & Souppaya, M. (2009). *Guide to enterprise password management.* Retrieved from NIST Special Publication 800-118: https://csrc.nist.gov/publications/detail/sp/800-118/archive/2009-04-21