|  |  |  |
| --- | --- | --- |
| **NOC REPORTING TEMPLATE** | | |
| Date Updated: 10/31/2022 | Name: Seke A. Moma | |
| ***A. Introduction*** | | |
| The Board of Directors for Psinuvia has requested that multiple scans be conducted on the company’s internal system in order to validate the company’s security. This was requested after a multitude of web exploits were recently reported in the news. As a result, a security assessment of the internal system will be conducted in addition to the daily routine scan schedule. The incident response team is in charge of this task and the following was discovered:   1. Host (172.20.1.131 was being attacked by SQL injection due to a vulnerability presented by a backend database via an Apache Web Server. 2. After examining said host/device it was concluded that multiple attempts were conducted to exploit the internal database via SQL injection attack, exploitation of the webserver (Apache), and Cross-Site Script (XXS) (AlienVault: I.T Security Report, “2020). | | |
| ***B. Scan Summary*** | | |
| The scan found several vulnerabilities (via Security Vulnerability Report) on host 172.20.1.131. measured as 4 serious, 32 high, 8 medium, and 1 low-level vulnerability (AlienVault: I.T Security Report, “2020).    Apache HTTP Server< 2.4.39 URL Normalization Vulnerability (Windows) outdated version 2.4.37 (Risk: High)  Mail server is answering to VRFY and EXPN requests (asking for information about an address Risk: High)  FTP unencrypted cleartext login (remote host is running an FTP service that accepts cleartext logins over unencrypted connections Risk: Medium).  IMAP unencrypted cleartext logins (remote host is running an FTP service that accepts cleartext logins over unencrypted connections Risk: Medium).  POP3 unencrypted cleartext logins (remote host is running an FTP service that accepts cleartext logins over unencrypted connections Risk: Medium).   * Microsoft SMB server vulnerabilities (Risk: serious) * Multiple OpenSSL issues (has reached EOL detection Risk: Serious)   Several PHP Issues   * EOL detection (Windows) Risk: Serious   Expired SSL/TLS Certificate   * SSL certificate using a weak signature algorithm (Risk: medium)   Timing vulnerability in DSA signature generation (CVE-2018-0734 (Windows) (Risk: medium)  HTTP TRACE XSS attach vulnerability (Risk: high)   * Debugging functions are enabled on the remote web server. * TRACE and TRACK are HTTP methods used to debug web server connections, and the web server is currently supporting these methods (AlienVault: I.T Security Report, “2020).   **Basic Assessment Questions**:   * Has the information been confirmed to be correct and accurate?   The reported SQL injection attempt occurred on host 172.20.1.131and has been confirmed via the vulnerability scanner, Zenmap scan results, and Alien Vault OSSIM outputs.   * Who, what, when, where, why, and how?   Who: the database connected to a PHP web-application (host 172.20.1.131).  What: SQL injection attempts  When: Zenmap scan @ 2021-09-13 19:48 CDT and Alien Vault OSSIM @ 2020-1-24 22:36:41  Why: still investigating  How: unfiltered/unmodified SQL statements sent to the database.   * What information is available from the firewall, router, server, system, intrusion detection system (IDS), system logs, etc.?   Still investigating.   * What type of data is involved, and what is its classification?   The data is from the effected database using unauthorized SQL commands. The structure of this data is unknown but is assumed to be business related or possibly patient information which is classified as sensitive.   * Are there obscenities, child pornography, or confrontational data?   The data is assumed to be business-related, there are currently no data to verify this indication of illegal information.   * Is there criminal activity?   Still investigating. There is no clear indication that any sensitive information has been successfully extracted by the discovered SQL injection attempts.   * Is the data protected by an encryption solution?   No, the data is being transmitted using cleartext over unencrypted connections. To the web application and from the web application to the database.   * What is the magnitude of the systems being impacted?   High magnitude   * Is the event still in progress?   Still investigating.   * Has preliminary containment been performed (i.e., disable account, reset password, remove remote access, isolate device in segregated segment)?   Specific accounts that could be disabled or removed were not located in order to prevent the above attack. The main thing to do here is to contain the incident by removing the above host and database from the existing network as mentioned in industry best practices.   * What is the estimated value of the impacted data and systems?   Still investigating (currently no data has been lost due to the unsuccessful attack attempts).  The requested security validation scan (Network Operations Center (NOC) for Psinuvia) confirms the above scan summary. Information was also retrieved from Zenmap and AlienVault OSSIM scans included in the documentation. The scans could not verify if the transmitted data was encrypted, but it was revealed that POP3, IMAP, and FTP are using unencrypted cleartext logins. In summary, this server has multiple vulnerabilities that could be exploited by a cybercriminal and require immediate remediation through several patches and updates. | | |
| ***C. Detailed Analysis*** | | |
| 1. Determine whether the vulnerability could apply to the system (e.g., check software list).   The vulnerability applies directly to the system using SQL commands.   1. Determine if the vulnerability is present on the system.   The vulnerability is present in the form of a SQL injection.   1. Determine whether the vulnerability could be exploited on the system(s) in question (e.g., vulnerability scans).   Yes the vulnerability could be exploited on the system due to the fact that the system is currently using plaintext HTTP connection to transmit information.   1. Validate whether or not the vulnerability has been exploited on the system (e.g., check logs).   Despite the fact that the system currently has several vulnerabilities with cleartext logins over unencrypted connections as well as SQL injection attempts, there is no evidence of successful extraction of sensitive information from the system.   1. Report findings to senior management through the use of the “NOC Reporting Template” (feel free to make modifications as the situation warrants). | | |
| ***D. Scan Response*** | | |
| The severity level of this security event/ scan is **high** due to the following:   * Unsuccessful SQL injection attempts of compromising sensitive data (the type of data being compromised is not evident based on the scans/alarm report, but Psainuvia is at risk of compromised sensitive business information and patient PII and HIPAA information) (“Alarm Report,” 2019-2020). * Potential loss of encrypted sensitive data (several cleartext logins over unencrypted connections). * Higher-than-normal level of intruder scanning and probing activities (984.749 alarm occurrences). * Damages to Psinuvia’s operations with potential legal liabilities (patient information breach).   Despite the lack of a successful SQL injection, the following personnel to be alerted within 4 hours while maintaining a provable chain of custody log during the assessment of the situation. CSIRT must ensure that all handoffs must be recorded with storage and transfer evidence between departments/parties.  **The chain of custody/ process of escalation:**  CTO 🡪 CISO 🡪 Director of Security Ops 🡪 Legal (per Incident Response Plan)  **CSIRT should maintain the following ongoing communication requirement:**  Once the incident update is sent to the CISO an incident update should be sent daily during the critical phase and weekly during the resolution phase. | | |
| ***E. Remediation*** | | |
| Because this is a productive serve with exposed vulnerability, it is prominent to remediate these security vulnerabilities immediately and efficiently. The first step of the action plan is to develop a containment strategy. Best practices suggest to “define acceptable risks in dealing with incidents and developing strategies accordingly” (Cichonski et al., 2012). (The effected device (host 172.20.1.131) should be shut down and removed from the network for continued remediation/patches and updates preferably during a scheduled maintenance period. After the host is taken offline a defense-in-depth approach should be utilized to combat and prevent SQL injection attacks/attempts. The database should then be configured to use preprocessed statements, along with input sanitization (whitelisting and/ or blacklisting) (Chapple et al., 2022). The update of both PHP and POP3 software is critical to enfore the latest versions/patches for the vulnerabilities discovered above (“Cybersecurity Incident Response Plan, “n.d.).  Service availability will be affected. It should be noted that FTP and mail will be unavailable, therefore remediation should be scheduled during non-business hours.  Next, as highlighted in the Incident Response Plan, the host should undergo an incident handling process in order to prioritize the handling of the incident and “lesson learned” meetings that will improve security measures (Cichonski et al., 2012).  Software should be patched through a patch management software such as SCCM, (as highlighted as industry best practices) this will ensure that the system is kept up t date with current patches. The patch management software should be effective in evaluating, testing, approving, and deploying patches, this effectiveness should be proven via system audits (Chapple et al., 2022). | | |
| ***F. Recommendations*** | | |
| Administrative Controls:   * A vulnerability scan should be scheduled quarterly in addition to regular intrusion scanning schedule. * All applications/software should be reviewed periodically, and versioning should be verified to prevent EOL detection. * SSL certificate renewals must be documented and reviewed quarterly to prevent expiration. | | Technical Controls:   * All POP3/FTP/SMTP/IMAP systems should exclusively use SSL OR TLS to ensure logins are not transmitted over unencrypted internet connections or in clear text. * A firewall that can block Denial of Service attacks should be implemented to prevent exploitation of vulnerabilities across the network. * SSL Forward Proxy decryption should also be implemented as an extra layering remediation tactic so the firewall can prevent threats in outbound traffic across the network. |

**References**

AlienVault: I.T Security Vulnerability Report. (2020)

Cichonski, P., Millar, T., Grance, T., &amp; Scarfone, K. (2012, August). Computer Security Incident Handling Guide. National Institute of Standard and Technology

I.T. Security. (2019-2020). Alarms Report

Psinuvia. (n.d.). Cybersecurity Incident Response Plan