Vulnerability Remediation Recommendations

CSA217.com

Created by: Patrick Murphy, Vulnerability Assessor

Reviewed by: Arsalan Parsaei, Professor

Approved by: Arsalan Parsaei, Manager

It is recommended that all vulnerabilities labelled as critical by Nessus and all vulnerabilities with a CVSS score greater than 7.0 should be remedied. The following are all discovered vulnerabilities meeting these criteria, and recommendations to solve these flaws to protect our MSP2 server. Not that all entries with a CVSS of NA are labelled as “High” or “Critical.”

1. **CVSS 10.0 - Unix Operating System Unsupported Version Detection**
   The operating system on the MSP2 server is no longer supported by the vendor. It should be updated to the latest version.
2. **CVSS 9.8 – PHP MyAdmin prior to 4.8.6 SQLi vulnerability (PMASA-2019-3)**
   The PHP MyAdmin version on the server is vulnerable to SQL injection. It should be upgraded to version 4.8.6 or later.
3. **CVSS 9.8 - Apache Tomcat AJP Connector Request Injection (Ghostcat)**
   A file vulnerability was discovered that allows an attacker to read sensitive files from the server. If allowed, they may also write files and perform remote code execution. The Tomcat server should be upgraded to 7.0.100, 8.5.51, 9.0.31 or later.
4. **CVSS 9.8 - Bind Shell Backdoor Detection**
   A remote port has a shell listening to it that does not require authentication, which could be used by an attacker to send commands directly to the system. It should be checked for indicators of compromise and authentication should be added.
5. **CVSS NA - Debian OpenSSH/OpenSSL Package Random Number Generator Weakness**
   The SSH keys used on the host were generated with a vulnerable random number generator, allowing attackers to obtain private keys. All cryptographic material on the server should be considered compromised and re-encrypted.
6. **CVSS NA - Debian OpenSSH/OpenSSL Package Random Number Generator Weakness (SSL check)**
   The X509 certificate on the server has been created with compromised random number generation and an attacker can obtain the private key. All cryptographic material on the server should be considered compromised and new keys should be made.
7. **CVSS NA - NFS Exported Share Information Disclosure**
   NFS shares can be accessed, allowing attackers to perform read/write operations of the MSL2 server. It should be configured for authorized users only.
8. **CVSS NA - VNC Server 'password' Password**
   The VNC server running on the host uses a weak password guessable by a hacker. It should be reconfigured to use a strong password.
9. **CVSS 8.8 - Apache PHP-CGI Remote Code Execution**
   The version of PHP on MSL2 allows arbitrary code execution. It should be updated to PHP 5.3.13 / 5.4.3 or later.
10. **CVSS 8.8 - TWiki 'rev' Parameter Arbitrary Command Execution**
    The server is hosting a version of TWiki that has an arbitrary command execution vulnerability. It should be upgraded with the vendor’s hotfix.
11. **CVSS 8.6 - ISC BIND Service Downgrade / Reflected DoS**
    The instance of ISC BIND running on MSL2 can be affected by service downgrade attacks. It should be upgraded to the current version.
12. **CVSS 7.5 - ISC BIND Denial of Service**

The ISC BIND on the server contains a vulnerability to DoS attacks. It should be upgraded to the most current version.

13. **CVSS 7.5 - NFS Shares World Readable**
    The MSL2 server is exporting shares without restricting access to force authorization. The configuration should be changed to place appropriate restrictions on shares.
14. **CVSS 7.5 - SSL Medium Strength Cipher Suites Supported (SWEET32)**
    The server will accept medium strength SSL ciphers, making it easier for attackers to decrypt information. It should be reconfigured to only accept strong SSL ciphers.
15. **CVSS 7.5 - SSL Version 2 and 3 Protocol Detection**
    The server accepts SSL versions 2 and 3, which have many vulnerabilities that can be taken advantage of. It should be configured to use TLS1.2 or higher.
16. **CVSS 7.5 - Samba Badlock Vulnerability**
    A vulnerability in the version of Samba could allow an attacker to see sensitive information or disable critical services. It should be updated to version 4.2.11 / 4.3.8 / 4.4.2 or later.
17. **CVSS NA - CGI Generic Remote File Inclusion**
    Scripts on the server fail to sanitize their inputs. Appropriate restrictions should be placed on the CGI application.
18. **CVSS NA - PHP PHP-CGI Query String Parameter Injection Arbitrary Code Execution**
    The version of PHP running allows arbitrary code execution. It should be upgraded to PHP 5.3.13 / 5.4.3 or later.
19. **phpMyAdmin Setup Script Configuration Parameters Arbitrary PHP Code Injection (PMASA-2009-4)**
    The version of PHP running has a code execution vulnerability. It should be upgraded to phpMyAdmin 3.1.3.2.