

**1. NFS Exported Share Information Disclosure**

|  |  |
| --- | --- |
| **Risk** | **Critical** |
| **Affected Hosts** | **192.168.60.131:2049** |
| **References** | **CVE-1999-0170** |
| **Description** | |
| At least one of the NFS shares exported by the remote server could be mounted by the scanning host. An attacker may be able to leverage this to read (and possibly write) files on remote host. | |
| **Recommendations** | |
| Configure NFS on the remote host so that only authorized hosts can mount its remote shares. | |

**2. SSL Version 2 and 3 Protocol Detection**

|  |  |
| --- | --- |
| **Risk** | **Critical** |
| **Affected Hosts** | **192.168.60.131:5432, 192.168.60.131:25** |
| **References** | **n/a** |
| **Description** | |
| The remote service accepts connections encrypted using SSL 2.0 and/or SSL 3.0. These versions of SSL are affected by several cryptographic flaws, including:   - An insecure padding scheme with CBC ciphers.   - Insecure session renegotiation and resumption schemes.  An attacker can exploit these flaws to conduct man-in-the-middle attacks or to decrypt communications between the affected service and clients.  Although SSL/TLS has a secure means for choosing the highest supported version of the protocol (so that these versions will be used only if the client or server support nothing better), many web browsers implement this in an unsafe way that allows an attacker to downgrade a connection (such as in POODLE). Therefore, it is recommended that these protocols be disabled entirely.  NIST has determined that SSL 3.0 is no longer acceptable for secure communications. As of the date of enforcement found in PCI DSS v3.1, any version of SSL will not meet the PCI SSC's definition of 'strong cryptography'. | |
| **Recommendations** | |
| Consult the application's documentation to disable SSL 2.0 and 3.0. Use TLS 1.2 (with approved cipher suites) or higher instead. | |

**3. Debian OpenSSH/OpenSSL Package Random Number Generator Weakness**

|  |  |
| --- | --- |
| **Risk** | **Critical** |
| **Affected Hosts** | **192.168.60.131:22** |
| **References** | **CVE-2008-0166** |
| **Description** | |
| The remote SSH host key has been generated on a Debian  or Ubuntu system which contains a bug in the random number generator of its OpenSSL library.  The problem is due to a Debian packager removing nearly all sources of entropy in the remote version of OpenSSL.  An attacker can easily obtain the private part of the remote key and use this to set up decipher the remote session or set up a man in the middle attack. | |
| **Recommendations** | |
| Consider all cryptographic material generated on the remote host to be guessable. In particuliar, all SSH, SSL and OpenVPN key material should be re-generated. | |

**4. Debian OpenSSH/OpenSSL Package Random Number Generator Weakness (SSL check)**

|  |  |
| --- | --- |
| **Risk** | **Critical** |
| **Affected Hosts** | **192.168.60.131:5432, 192.168.60.131:25** |
| **References** | **CVE-2008-0166** |
| **Description** | |
| The remote x509 certificate on the remote SSL server has been generated on a Debian or Ubuntu system which contains a bug in the random number generator of its OpenSSL library.   The problem is due to a Debian packager removing nearly all sources of entropy in the remote version of OpenSSL.   An attacker can easily obtain the private part of the remote key and use this to decipher the remote session or set up a man in the middle attack. | |
| **Recommendations** | |
| Consider all cryptographic material generated on the remote host to be guessable. In particuliar, all SSH, SSL and OpenVPN key material should be re-generated. | |

**5. Unix Operating System Unsupported Version Detection**

|  |  |
| --- | --- |
| **Risk** | **Critical** |
| **Affected Hosts** | **192.168.60.131:0** |
| **References** | **n/a** |
| **Description** | |
| According to its self-reported version number, the Unix operating system running on the remote host is no longer supported.  Lack of support implies that no new security patches for the product will be released by the vendor. As a result, it is likely to contain security vulnerabilities. | |
| **Recommendations** | |
| Upgrade to a version of the Unix operating system that is currently supported. | |

**6. UnrealIRCd Backdoor Detection**

|  |  |
| --- | --- |
| **Risk** | **Critical** |
| **Affected Hosts** | **192.168.60.131:6667** |
| **References** | **CVE-2010-2075** |
| **Description** | |
| The remote IRC server is a version of UnrealIRCd with a backdoor that allows an attacker to execute arbitrary code on the affected host. | |
| **Recommendations** | |
| Re-download the software, verify it using the published MD5 / SHA1 checksums, and re-install it. | |

**7. Bind Shell Backdoor Detection**

|  |  |
| --- | --- |
| **Risk** | **Critical** |
| **Affected Hosts** | **192.168.60.131:1524** |
| **References** | **n/a** |
| **Description** | |
| A shell is listening on the remote port without any authentication being required. An attacker may use it by connecting to the remote port and sending commands directly. | |
| **Recommendations** | |
| Verify if the remote host has been compromised, and reinstall the system if necessary. | |

**8. VNC Server 'password' Password**

|  |  |
| --- | --- |
| **Risk** | **Critical** |
| **Affected Hosts** | **192.168.60.131:5900** |
| **References** | **n/a** |
| **Description** | |
| The VNC server running on the remote host is secured with a weak password. Nessus was able to login using VNC authentication and a password of 'password'. A remote, unauthenticated attacker could exploit this to take control of the system. | |
| **Recommendations** | |
| Secure the VNC service with a strong password. | |

**9. Apache PHP-CGI Remote Code Execution**

|  |  |
| --- | --- |
| **Risk** | **Critical** |
| **Affected Hosts** | **192.168.60.131:80** |
| **References** | **CVE-2012-1823** |
| **Description** | |
| The PHP installation on the remote web server contains a flaw that could allow a remote attacker to pass command-line arguments as part of a query string to the PHP-CGI program. This could be abused to execute arbitrary code, reveal PHP source code, cause a system crash, etc. | |
| **Recommendations** | |
| Upgrade to PHP 5.3.13 / 5.4.3 or later. | |

**10. phpMyAdmin prior to 4.8.6 SQLi vulnerablity (PMASA-2019-3)**

|  |  |
| --- | --- |
| **Risk** | **Critical** |
| **Affected Hosts** | **192.168.60.131:80** |
| **References** | **CVE-2019-11768** |
| **Description** | |
| According to its self-reported version number, the phpMyAdmin application hosted on the remote web server is prior to 4.8.6. It is, therefore, affected by a SQL injection (SQLi) vulnerability that exists in designer feature of phpMyAdmin. An unauthenticated, remote attacker can exploit this to inject or manipulate SQL queries in the back-end database, resulting in the disclosure or manipulation of arbitrary data.  Note that Nessus has not attempted to exploit these issues but has instead relied only on the application's self-reported version number. | |
| **Recommendations** | |
| Upgrade to phpMyAdmin version 4.8.6 or later. Alternatively, apply the patches referenced in the vendor advisories. | |

**11. Apache Tomcat SEoL (<= 5.5.x)**

|  |  |
| --- | --- |
| **Risk** | **Critical** |
| **Affected Hosts** | **192.168.60.131:8180** |
| **References** | **n/a** |
| **Description** | |
| According to its version, Apache Tomcat is less than or equal to 5.5.x. It is, therefore, no longer maintained by its vendor or provider.  Lack of support implies that no new security patches for the product will be released by the vendor. As a result, it may contain security vulnerabilities. | |
| **Recommendations** | |
| Upgrade to a version of Apache Tomcat that is currently supported. | |

**12. rlogin Service Detection**

|  |  |
| --- | --- |
| **Risk** | **High** |
| **Affected Hosts** | **192.168.60.131:513** |
| **References** | **CVE-1999-0651** |
| **Description** | |
| The rlogin service is running on the remote host. This service is vulnerable since data is passed between the rlogin client and server in cleartext. A man-in-the-middle attacker can exploit this to sniff logins and passwords. Also, it may allow poorly authenticated logins without passwords. If the host is vulnerable to TCP sequence number guessing (from any network) or IP spoofing (including ARP hijacking on a local network) then it may be possible to bypass authentication. Finally, rlogin is an easy way to turn file-write access into full logins through the .rhosts or rhosts.equiv files. | |
| **Recommendations** | |
| Comment out the 'login' line in /etc/inetd.conf and restart the inetd process. Alternatively, disable this service and use SSH instead. | |

**13. rsh Service Detection**

|  |  |
| --- | --- |
| **Risk** | **High** |
| **Affected Hosts** | **192.168.60.131:514** |
| **References** | **CVE-1999-0651** |
| **Description** | |
| The rsh service is running on the remote host. This service is vulnerable since data is passed between the rsh client and server in cleartext. A man-in-the-middle attacker can exploit this to sniff logins and passwords. Also, it may allow poorly authenticated logins without passwords. If the host is vulnerable to TCP sequence number guessing (from any network) or IP spoofing (including ARP hijacking on a local network) then it may be possible to bypass authentication. Finally, rsh is an easy way to turn file-write access into full logins through the .rhosts or rhosts.equiv files. | |
| **Recommendations** | |
| Comment out the 'rsh' line in /etc/inetd.conf and restart the inetd process. Alternatively, disable this service and use SSH instead. | |

**14. TWiki 'rev' Parameter Arbitrary Command Execution**

|  |  |
| --- | --- |
| **Risk** | **High** |
| **Affected Hosts** | **192.168.60.131:80** |
| **References** | **CVE-2005-2877** |
| **Description** | |
| The version of TWiki running on the remote host allows an attacker to manipulate input to the 'rev' parameter in order to execute arbitrary shell commands on the remote host subject to the privileges of the web server user id. | |
| **Recommendations** | |
| Apply the appropriate hotfix referenced in the vendor advisory. | |

**15. phpMyAdmin Setup Script Configuration Parameters Arbitrary PHP Code Injection (PMASA-2009-4)**

|  |  |
| --- | --- |
| **Risk** | **High** |
| **Affected Hosts** | **192.168.60.131:80** |
| **References** | **CVE-2009-1285** |
| **Description** | |
| The setup script included with the version of phpMyAdmin installed on the remote host does not properly sanitize user-supplied input before using it to generate a config file for the application. This version is affected by the following vulnerabilities :   - The setup script inserts the unsanitized verbose server   name into a C-style comment during config file   generation.   - An attacker can save arbitrary data to the generated   config file by altering the value of the 'textconfig'   parameter during a POST request to config.php.  An unauthenticated, remote attacker can exploit these issues to execute arbitrary PHP code. | |
| **Recommendations** | |
| Upgrade to phpMyAdmin 3.1.3.2. Alternatively, apply the patches referenced in the project's advisory. | |

**16. CGI Generic Remote File Inclusion**

|  |  |
| --- | --- |
| **Risk** | **High** |
| **Affected Hosts** | **192.168.60.131:80** |
| **References** | **n/a** |
| **Description** | |
| The remote web server hosts CGI scripts that fail to adequately sanitize  request strings. By leveraging this issue, an attacker may be able  to include a remote file from a remote server and execute arbitrary  commands on the target host. | |
| **Recommendations** | |
| Restrict access to the vulnerable application. Contact the vendor  for a patch or upgrade. | |

**17. NFS Shares World Readable**

|  |  |
| --- | --- |
| **Risk** | **High** |
| **Affected Hosts** | **192.168.60.131:2049** |
| **References** | **n/a** |
| **Description** | |
| The remote NFS server is exporting one or more shares without restricting access (based on hostname, IP, or IP range). | |
| **Recommendations** | |
| Place the appropriate restrictions on all NFS shares. | |

**18. SSL Medium Strength Cipher Suites Supported (SWEET32)**

|  |  |
| --- | --- |
| **Risk** | **High** |
| **Affected Hosts** | **192.168.60.131:5432, 192.168.60.131:25** |
| **References** | **CVE-2016-2183** |
| **Description** | |
| The remote host supports the use of SSL ciphers that offer medium strength encryption. Nessus regards medium strength as any encryption that uses key lengths at least 64 bits and less than 112 bits, or  else that uses the 3DES encryption suite.  Note that it is considerably easier to circumvent medium strength encryption if the attacker is on the same physical network. | |
| **Recommendations** | |
| Reconfigure the affected application if possible to avoid use of medium strength ciphers. | |

**19. PHP PHP-CGI Query String Parameter Injection Arbitrary Code Execution**

|  |  |
| --- | --- |
| **Risk** | **High** |
| **Affected Hosts** | **192.168.60.131:80** |
| **References** | **CVE-2012-1823** |
| **Description** | |
| The PHP installation on the remote web server contains a flaw that could allow a remote attacker to pass command-line arguments as part of a query string to the PHP-CGI program. This could be abused to execute arbitrary code, reveal PHP source code, cause a system crash, etc. | |
| **Recommendations** | |
| If using Lotus Foundations, upgrade the Lotus Foundations operating system to version 1.2.2b or later.   Otherwise, upgrade to PHP 5.3.13 / 5.4.3 or later. | |

**20. Samba Badlock Vulnerability**

|  |  |
| --- | --- |
| **Risk** | **High** |
| **Affected Hosts** | **192.168.60.131:445** |
| **References** | **CVE-2016-2118** |
| **Description** | |
| The version of Samba, a CIFS/SMB server for Linux and Unix, running on the remote host is affected by a flaw, known as Badlock, that exists in the Security Account Manager (SAM) and Local Security Authority (Domain Policy) (LSAD) protocols due to improper authentication level negotiation over Remote Procedure Call (RPC) channels. A man-in-the-middle attacker who is able to able to intercept the traffic between a client and a server hosting a SAM database can exploit this flaw to force a downgrade of the authentication level, which allows the execution of arbitrary Samba network calls in the context of the intercepted user, such as viewing or modifying sensitive security data in the Active Directory (AD) database or disabling critical services. | |
| **Recommendations** | |
| Upgrade to Samba version 4.2.11 / 4.3.8 / 4.4.2 or later. | |

**21. ISC BIND Service Downgrade / Reflected DoS**

|  |  |
| --- | --- |
| **Risk** | **High** |
| **Affected Hosts** | **192.168.60.131:53** |
| **References** | **CVE-2020-8616** |
| **Description** | |
| According to its self-reported version, the instance of ISC BIND 9 running on the remote name server is affected by performance downgrade and Reflected DoS vulnerabilities. This is due to BIND DNS not sufficiently limiting the number fetches which may be performed while processing a referral response.  An unauthenticated, remote attacker can exploit this to cause degrade the service of the recursive server or to use the affected server as a reflector in a reflection attack. | |
| **Recommendations** | |
| Upgrade to the ISC BIND version referenced in the vendor advisory. | |

**22. HTTP TRACE / TRACK Methods Allowed**

|  |  |
| --- | --- |
| **Risk** | **Medium** |
| **Affected Hosts** | **192.168.60.131:80** |
| **References** | **CVE-2003-1567** |
| **Description** | |
| The remote web server supports the TRACE and/or TRACK methods. TRACE and TRACK are HTTP methods that are used to debug web server connections. | |
| **Recommendations** | |
| Disable these HTTP methods. Refer to the plugin output for more information. | |

**23. Web Server info.php / phpinfo.php Detection**

|  |  |
| --- | --- |
| **Risk** | **Medium** |
| **Affected Hosts** | **192.168.60.131:80** |
| **References** | **n/a** |
| **Description** | |
| Many PHP installation tutorials instruct the user to create a PHP file that calls the PHP function 'phpinfo()' for debugging purposes.  Various PHP applications may also include such a file. By accessing such a file, a remote attacker can discover a large amount of information about the remote web server, including :   - The username of the user who installed PHP and if they  are a SUDO user.   - The IP address of the host.   - The version of the operating system.   - The web server version.   - The root directory of the web server.    - Configuration information about the remote PHP   installation. | |
| **Recommendations** | |
| Remove the affected file(s). | |

**24. Backup Files Disclosure**

|  |  |
| --- | --- |
| **Risk** | **Medium** |
| **Affected Hosts** | **192.168.60.131:80** |
| **References** | **n/a** |
| **Description** | |
| By appending various suffixes (ie: .old, .bak, ~, etc...) to the names of various files on the remote host, it seems possible to retrieve their contents, which may result in disclosure of sensitive information. | |
| **Recommendations** | |
| Ensure the files do not contain any sensitive information, such as credentials to connect to a database, and delete or protect those files that should not be accessible. | |

**25. Apache Tomcat Default Files**

|  |  |
| --- | --- |
| **Risk** | **Medium** |
| **Affected Hosts** | **192.168.60.131:8180** |
| **References** | **n/a** |
| **Description** | |
| The default error page, default index page, example JSPs and/or example servlets are installed on the remote Apache Tomcat server. These files should be removed as they may help an attacker uncover information about the remote Tomcat install or host itself. | |
| **Recommendations** | |
| Delete the default index page and remove the example JSP and servlets. Follow the Tomcat or OWASP instructions to  replace or modify the default error page. | |

**26. DNS Server Cache Snooping Remote Information Disclosure**

|  |  |
| --- | --- |
| **Risk** | **Medium** |
| **Affected Hosts** | **192.168.60.131:53** |
| **References** | **n/a** |
| **Description** | |
| The remote DNS server responds to queries for third-party domains that do not have the recursion bit set.   This may allow a remote attacker to determine which domains have recently been resolved via this name server, and therefore which hosts have been recently visited.   For instance, if an attacker was interested in whether your company utilizes the online services of a particular financial institution, they would be able to use this attack to build a statistical model regarding company usage of that financial institution. Of course, the attack can also be used to find B2B partners, web-surfing patterns, external mail servers, and more.  Note: If this is an internal DNS server not accessible to outside networks, attacks would be limited to the internal network. This may include employees, consultants and potentially users on a guest network or WiFi connection if supported. | |
| **Recommendations** | |
| Contact the vendor of the DNS software for a fix. | |

**27. SSL Certificate Expiry**

|  |  |
| --- | --- |
| **Risk** | **Medium** |
| **Affected Hosts** | **192.168.60.131:5432, 192.168.60.131:25** |
| **References** | **n/a** |
| **Description** | |
| This plugin checks expiry dates of certificates associated with SSL- enabled services on the target and reports whether any have already expired. | |
| **Recommendations** | |
| Purchase or generate a new SSL certificate to replace the existing one. | |

**28. SSL Weak Cipher Suites Supported**

|  |  |
| --- | --- |
| **Risk** | **Medium** |
| **Affected Hosts** | **192.168.60.131:25** |
| **References** | **n/a** |
| **Description** | |
| The remote host supports the use of SSL ciphers that offer weak encryption.  Note: This is considerably easier to exploit if the attacker is on the same physical network. | |
| **Recommendations** | |
| Reconfigure the affected application, if possible to avoid the use of weak ciphers. | |

**29. SSL Anonymous Cipher Suites Supported**

|  |  |
| --- | --- |
| **Risk** | **Medium** |
| **Affected Hosts** | **192.168.60.131:25** |
| **References** | **CVE-2007-1858** |
| **Description** | |
| The remote host supports the use of anonymous SSL ciphers. While this enables an administrator to set up a service that encrypts traffic without having to generate and configure SSL certificates, it offers no way to verify the remote host's identity and renders the service vulnerable to a man-in-the-middle attack.  Note: This is considerably easier to exploit if the attacker is on the same physical network. | |
| **Recommendations** | |
| Reconfigure the affected application if possible to avoid use of weak ciphers. | |

**30. Multiple Vendor DNS Query ID Field Prediction Cache Poisoning**

|  |  |
| --- | --- |
| **Risk** | **Medium** |
| **Affected Hosts** | **192.168.60.131:53** |
| **References** | **CVE-2008-1447** |
| **Description** | |
| The remote DNS resolver does not use random ports when making queries to third-party DNS servers. An unauthenticated, remote attacker can exploit this to poison the remote DNS server, allowing the attacker to divert legitimate traffic to arbitrary sites. | |
| **Recommendations** | |
| Contact your DNS server vendor for a patch. | |

**31. phpMyAdmin file\_path Parameter Vulnerabilities (PMASA-2009-1)**

|  |  |
| --- | --- |
| **Risk** | **Medium** |
| **Affected Hosts** | **192.168.60.131:80** |
| **References** | **n/a** |
| **Description** | |
| The version of phpMyAdmin installed on the remote host fails to sanitize user-supplied input to the 'file\_path' parameter of the 'bs\_disp\_as\_mime\_type.php' script before using it to read a file and reporting it in dynamically-generated HTML. An unauthenticated, remote attacker may be able to leverage this issue to read arbitrary files, possibly from third-party hosts, or to inject arbitrary HTTP headers in responses sent to third-party users.  Note that the application is also reportedly affected by several other issues, although Nessus has not actually checked for them. | |
| **Recommendations** | |
| Upgrade to phpMyAdmin 3.1.3.1 or apply the patch referenced in the project's advisory. | |

**32. Browsable Web Directories**

|  |  |
| --- | --- |
| **Risk** | **Medium** |
| **Affected Hosts** | **192.168.60.131:80** |
| **References** | **n/a** |
| **Description** | |
| Multiple Nessus plugins identified directories on the web server that are browsable. | |
| **Recommendations** | |
| Make sure that browsable directories do not leak confidential information or give access to sensitive resources. Additionally, use access restrictions or disable directory indexing for any that do. | |

**33. Unencrypted Telnet Server**

|  |  |
| --- | --- |
| **Risk** | **Medium** |
| **Affected Hosts** | **192.168.60.131:23** |
| **References** | **n/a** |
| **Description** | |
| The remote host is running a Telnet server over an unencrypted channel.  Using Telnet over an unencrypted channel is not recommended as logins, passwords, and commands are transferred in cleartext. This allows a  remote, man-in-the-middle attacker to eavesdrop on a Telnet session to obtain credentials or other sensitive information and to modify traffic exchanged between a client and server.  SSH is preferred over Telnet since it protects credentials from eavesdropping and can tunnel additional data streams such as an X11 session. | |
| **Recommendations** | |
| Disable the Telnet service and use SSH instead. | |

**34. SSL Certificate with Wrong Hostname**

|  |  |
| --- | --- |
| **Risk** | **Medium** |
| **Affected Hosts** | **192.168.60.131:5432, 192.168.60.131:25** |
| **References** | **n/a** |
| **Description** | |
| The 'commonName' (CN) attribute of the SSL certificate presented for this service is for a different machine. | |
| **Recommendations** | |
| Purchase or generate a proper SSL certificate for this service. | |

**35. PHP expose\_php Information Disclosure**

|  |  |
| --- | --- |
| **Risk** | **Medium** |
| **Affected Hosts** | **192.168.60.131:80** |
| **References** | **n/a** |
| **Description** | |
| The PHP install on the remote server is configured in a way that allows disclosure of potentially sensitive information to an attacker through a special URL. Such a URL triggers an Easter egg built into PHP itself.   Other such Easter eggs likely exist, but Nessus has not checked for them. | |
| **Recommendations** | |
| In the PHP configuration file, php.ini, set the value for 'expose\_php' to 'Off' to disable this behavior. Restart the web server daemon to put this change into effect. | |

**36. phpMyAdmin setup.php Verbose Server Name XSS (PMASA-2010-7)**

|  |  |
| --- | --- |
| **Risk** | **Medium** |
| **Affected Hosts** | **192.168.60.131:80** |
| **References** | **CVE-2010-3263** |
| **Description** | |
| The setup script included with the version of phpMyAdmin installed on the remote host does not properly sanitize user-supplied input to the 'verbose server name' field.  A remote attacker could exploit this by tricking a user into executing arbitrary script code. | |
| **Recommendations** | |
| Upgrade to phpMyAdmin 3.3.7 or later. | |

**37. SSL Certificate Cannot Be Trusted**

|  |  |
| --- | --- |
| **Risk** | **Medium** |
| **Affected Hosts** | **192.168.60.131:5432, 192.168.60.131:25** |
| **References** | **n/a** |
| **Description** | |
| The server's X.509 certificate cannot be trusted. This situation can occur in three different ways, in which the chain of trust can be broken, as stated below :   - First, the top of the certificate chain sent by the  server might not be descended from a known public  certificate authority. This can occur either when the  top of the chain is an unrecognized, self-signed  certificate, or when intermediate certificates are  missing that would connect the top of the certificate  chain to a known public certificate authority.   - Second, the certificate chain may contain a certificate  that is not valid at the time of the scan. This can  occur either when the scan occurs before one of the  certificate's 'notBefore' dates, or after one of the  certificate's 'notAfter' dates.   - Third, the certificate chain may contain a signature  that either didn't match the certificate's information  or could not be verified. Bad signatures can be fixed by  getting the certificate with the bad signature to be  re-signed by its issuer. Signatures that could not be  verified are the result of the certificate's issuer  using a signing algorithm that Nessus either does not  support or does not recognize.  If the remote host is a public host in production, any break in the chain makes it more difficult for users to verify the authenticity and  identity of the web server. This could make it easier to carry out  man-in-the-middle attacks against the remote host. | |
| **Recommendations** | |
| Purchase or generate a proper SSL certificate for this service. | |

**38. phpMyAdmin error.php BBcode Tag XSS (PMASA-2010-9)**

|  |  |
| --- | --- |
| **Risk** | **Medium** |
| **Affected Hosts** | **192.168.60.131:80** |
| **References** | **CVE-2010-4480** |
| **Description** | |
| The version of phpMyAdmin fails to validate BBcode tags in user input to the 'error' parameter of the 'error.php' script before using it to generate dynamic HTML.  An attacker may be able to leverage this issue to inject arbitrary HTML or script code into a user's browser to be executed within the security context of the affected site. For example, this could be used to cause a page with arbitrary text and a link to an external site to be displayed. | |
| **Recommendations** | |
| Upgrade to phpMyAdmin 3.4.0-beta1 or later. | |

**39. SMTP Service STARTTLS Plaintext Command Injection**

|  |  |
| --- | --- |
| **Risk** | **Medium** |
| **Affected Hosts** | **192.168.60.131:25** |
| **References** | **CVE-2011-0411** |
| **Description** | |
| The remote SMTP service contains a software flaw in its STARTTLS implementation that could allow a remote, unauthenticated attacker to inject commands during the plaintext protocol phase that will be executed during the ciphertext protocol phase.   Successful exploitation could allow an attacker to steal a victim's email or associated SASL (Simple Authentication and Security Layer) credentials. | |
| **Recommendations** | |
| Contact the vendor to see if an update is available. | |

**40. SSL Self-Signed Certificate**

|  |  |
| --- | --- |
| **Risk** | **Medium** |
| **Affected Hosts** | **192.168.60.131:5432, 192.168.60.131:25** |
| **References** | **n/a** |
| **Description** | |
| The X.509 certificate chain for this service is not signed by a recognized certificate authority. If the remote host is a public host in production, this nullifies the use of SSL as anyone could establish a man-in-the-middle attack against the remote host.   Note that this plugin does not check for certificate chains that end in a certificate that is not self-signed, but is signed by an unrecognized certificate authority. | |
| **Recommendations** | |
| Purchase or generate a proper SSL certificate for this service. | |

**41. SMB Signing not required**

|  |  |
| --- | --- |
| **Risk** | **Medium** |
| **Affected Hosts** | **192.168.60.131:445** |
| **References** | **n/a** |
| **Description** | |
| Signing is not required on the remote SMB server. An unauthenticated, remote attacker can exploit this to conduct man-in-the-middle attacks against the SMB server. | |
| **Recommendations** | |
| Enforce message signing in the host's configuration. On Windows, this is found in the policy setting 'Microsoft network server: Digitally sign communications (always)'. On Samba, the setting is called 'server signing'. See the 'see also' links for further details. | |

**42. Web Application Information Disclosure**

|  |  |
| --- | --- |
| **Risk** | **Medium** |
| **Affected Hosts** | **192.168.60.131:80** |
| **References** | **n/a** |
| **Description** | |
| At least one web application hosted on the remote web server discloses the physical path to its directories when a malformed request is sent to it.  Leaking this kind of information may help an attacker fine-tune attacks against the application and its backend. | |
| **Recommendations** | |
| Filter error messages containing path information. | |

**43. SSL RC4 Cipher Suites Supported (Bar Mitzvah)**

|  |  |
| --- | --- |
| **Risk** | **Medium** |
| **Affected Hosts** | **192.168.60.131:5432, 192.168.60.131:25** |
| **References** | **CVE-2013-2566** |
| **Description** | |
| The remote host supports the use of RC4 in one or more cipher suites. The RC4 cipher is flawed in its generation of a pseudo-random stream of bytes so that a wide variety of small biases are introduced into the stream, decreasing its randomness.  If plaintext is repeatedly encrypted (e.g., HTTP cookies), and an attacker is able to obtain many (i.e., tens of millions) ciphertexts, the attacker may be able to derive the plaintext. | |
| **Recommendations** | |
| Reconfigure the affected application, if possible, to avoid use of RC4 ciphers. Consider using TLS 1.2 with AES-GCM suites subject to browser and web server support. | |

**44. SSL/TLS EXPORT\_RSA <= 512-bit Cipher Suites Supported (FREAK)**

|  |  |
| --- | --- |
| **Risk** | **Medium** |
| **Affected Hosts** | **192.168.60.131:25** |
| **References** | **CVE-2015-0204** |
| **Description** | |
| The remote host supports EXPORT\_RSA cipher suites with keys less than or equal to 512 bits. An attacker can factor a 512-bit RSA modulus in a short amount of time.  A man-in-the middle attacker may be able to downgrade the session to use EXPORT\_RSA cipher suites (e.g. CVE-2015-0204). Thus, it is recommended to remove support for weak cipher suites. | |
| **Recommendations** | |
| Reconfigure the service to remove support for EXPORT\_RSA cipher suites. | |

**45. Web Application Potentially Vulnerable to Clickjacking**

|  |  |
| --- | --- |
| **Risk** | **Medium** |
| **Affected Hosts** | **192.168.60.131:80, 192.168.60.131:8180** |
| **References** | **n/a** |
| **Description** | |
| The remote web server does not set an X-Frame-Options response header or a Content-Security-Policy 'frame-ancestors' response header in all content responses. This could potentially expose the site to a clickjacking or UI redress attack, in which an attacker can trick a user into clicking an area of the vulnerable page that is different than what the user perceives the page to be. This can result in a user performing fraudulent or malicious transactions.  X-Frame-Options has been proposed by Microsoft as a way to mitigate clickjacking attacks and is currently supported by all major browser vendors.  Content-Security-Policy (CSP) has been proposed by the W3C Web Application Security Working Group, with increasing support among all major browser vendors, as a way to mitigate clickjacking and other attacks. The 'frame-ancestors' policy directive restricts which sources can embed the protected resource.  Note that while the X-Frame-Options and Content-Security-Policy response headers are not the only mitigations for clickjacking, they are currently the most reliable methods that can be detected through automation. Therefore, this plugin may produce false positives if other mitigation strategies (e.g., frame-busting JavaScript) are deployed or if the page does not perform any security-sensitive transactions. | |
| **Recommendations** | |
| Return the X-Frame-Options or Content-Security-Policy (with the 'frame-ancestors' directive) HTTP header with the page's response. This prevents the page's content from being rendered by another site when using the frame or iframe HTML tags. | |

**46. SSL DROWN Attack Vulnerability (Decrypting RSA with Obsolete and Weakened eNcryption)**

|  |  |
| --- | --- |
| **Risk** | **Medium** |
| **Affected Hosts** | **192.168.60.131:25** |
| **References** | **CVE-2016-0800** |
| **Description** | |
| The remote host supports SSLv2 and therefore may be affected by a vulnerability that allows a cross-protocol Bleichenbacher padding oracle attack known as DROWN (Decrypting RSA with Obsolete and Weakened eNcryption). This vulnerability exists due to a flaw in the Secure Sockets Layer Version 2 (SSLv2) implementation, and it allows captured TLS traffic to be decrypted. A man-in-the-middle attacker can exploit this to decrypt the TLS connection by utilizing previously captured traffic and weak cryptography along with a series of specially crafted connections to an SSLv2 server that uses the same private key. | |
| **Recommendations** | |
| Disable SSLv2 and export grade cryptography cipher suites. Ensure that private keys are not used anywhere with server software that supports SSLv2 connections. | |

**47. SSH Weak Algorithms Supported**

|  |  |
| --- | --- |
| **Risk** | **Medium** |
| **Affected Hosts** | **192.168.60.131:22** |
| **References** | **n/a** |
| **Description** | |
| Nessus has detected that the remote SSH server is configured to use the Arcfour stream cipher or no cipher at all. RFC 4253 advises against using Arcfour due to an issue with weak keys. | |
| **Recommendations** | |
| Contact the vendor or consult product documentation to remove the weak ciphers. | |

**48. TLS Version 1.0 Protocol Detection**

|  |  |
| --- | --- |
| **Risk** | **Medium** |
| **Affected Hosts** | **192.168.60.131:5432, 192.168.60.131:25** |
| **References** | **n/a** |
| **Description** | |
| The remote service accepts connections encrypted using TLS 1.0. TLS 1.0 has a number of cryptographic design flaws. Modern implementations of TLS 1.0 mitigate these problems, but newer versions of TLS like 1.2 and 1.3 are designed against these flaws and should be used whenever possible.  As of March 31, 2020, Endpoints that aren’t enabled for TLS 1.2 and higher will no longer function properly with major web browsers and major vendors.  PCI DSS v3.2 requires that TLS 1.0 be disabled entirely by June 30, 2018, except for POS POI terminals (and the SSL/TLS termination points to which they connect) that can be verified as not being susceptible to any known exploits. | |
| **Recommendations** | |
| Enable support for TLS 1.2 and 1.3, and disable support for TLS 1.0. | |

**49. ISC BIND Denial of Service**

|  |  |
| --- | --- |
| **Risk** | **Medium** |
| **Affected Hosts** | **192.168.60.131:53** |
| **References** | **CVE-2020-8617** |
| **Description** | |
| A denial of service (DoS) vulnerability exists in ISC BIND versions 9.11.18 / 9.11.18-S1 / 9.12.4-P2 / 9.13 / 9.14.11 / 9.15 / 9.16.2 / 9.17 / 9.17.1 and earlier. An unauthenticated, remote attacker can exploit this issue, via a specially-crafted message, to cause the service to stop responding.  Note that Nessus has not tested for this issue but has instead relied only on the application's self-reported version number. | |
| **Recommendations** | |
| Upgrade to the patched release most closely related to your current version of BIND. | |

**50. ISC BIND 9.x < 9.11.22, 9.12.x < 9.16.6, 9.17.x < 9.17.4 DoS**

|  |  |
| --- | --- |
| **Risk** | **Medium** |
| **Affected Hosts** | **192.168.60.131:53** |
| **References** | **CVE-2020-8622** |
| **Description** | |
| According to its self-reported version number, the installation of ISC BIND running on the remote name server is  version 9.x prior to 9.11.22, 9.12.x prior to 9.16.6 or 9.17.x prior to 9.17.4. It is, therefore, affected by a denial of service (DoS) vulnerability due to an assertion failure when attempting to verify a truncated response to a  TSIG-signed request. An authenticated, remote attacker can exploit this issue by sending a truncated response to a TSIG-signed request to trigger an assertion failure, causing the server to exit.  Note that Nessus has not tested for this issue but has instead relied only on the application's self-reported version  number. | |
| **Recommendations** | |
| Upgrade to BIND 9.11.22, 9.16.6, 9.17.4 or later. | |

**51. X Server Detection**

|  |  |
| --- | --- |
| **Risk** | **Low** |
| **Affected Hosts** | **192.168.60.131:6000** |
| **References** | **n/a** |
| **Description** | |
| The remote host is running an X11 server. X11 is a client-server protocol that can be used to display graphical applications running on a given host on a remote client.   Since the X11 traffic is not ciphered, it is possible for an attacker to eavesdrop on the connection. | |
| **Recommendations** | |
| Restrict access to this port. If the X11 client/server facility is not used, disable TCP support in X11 entirely (-nolisten tcp). | |

**52. Web Server Transmits Cleartext Credentials**

|  |  |
| --- | --- |
| **Risk** | **Low** |
| **Affected Hosts** | **192.168.60.131:80, 192.168.60.131:8180** |
| **References** | **n/a** |
| **Description** | |
| The remote web server contains several HTML form fields containing an input of type 'password' which transmit their information to a remote web server in cleartext.  An attacker eavesdropping the traffic between web browser and  server may obtain logins and passwords of valid users. | |
| **Recommendations** | |
| Make sure that every sensitive form transmits content over HTTPS. | |

**53. Web Server Uses Basic Authentication Without HTTPS**

|  |  |
| --- | --- |
| **Risk** | **Low** |
| **Affected Hosts** | **192.168.60.131:8180** |
| **References** | **n/a** |
| **Description** | |
| The remote web server contains web pages that are protected by 'Basic' authentication over cleartext.  An attacker eavesdropping the traffic might obtain logins and passwords of valid users. | |
| **Recommendations** | |
| Make sure that HTTP authentication is transmitted over HTTPS. | |

**54. Web Server Allows Password Auto-Completion**

|  |  |
| --- | --- |
| **Risk** | **Low** |
| **Affected Hosts** | **192.168.60.131:80, 192.168.60.131:8180** |
| **References** | **n/a** |
| **Description** | |
| The remote web server contains at least one HTML form field that has an input of type 'password' where 'autocomplete' is not set to 'off'.  While this does not represent a risk to this web server per se, it does mean that users who use the affected forms may have their credentials saved in their browsers, which could in turn lead to a loss of confidentiality if any of them use a shared host or if their machine is compromised at some point. | |
| **Recommendations** | |
| Add the attribute 'autocomplete=off' to these fields to prevent browsers from caching credentials. | |

**55. SSH Server CBC Mode Ciphers Enabled**

|  |  |
| --- | --- |
| **Risk** | **Low** |
| **Affected Hosts** | **192.168.60.131:22** |
| **References** | **CVE-2008-5161** |
| **Description** | |
| The SSH server is configured to support Cipher Block Chaining (CBC) encryption. This may allow an attacker to recover the plaintext message from the ciphertext.   Note that this plugin only checks for the options of the SSH server and does not check for vulnerable software versions. | |
| **Recommendations** | |
| Contact the vendor or consult product documentation to disable CBC mode cipher encryption, and enable CTR or GCM cipher mode encryption. | |

**56. SSH Weak MAC Algorithms Enabled**

|  |  |
| --- | --- |
| **Risk** | **Low** |
| **Affected Hosts** | **192.168.60.131:22** |
| **References** | **n/a** |
| **Description** | |
| The remote SSH server is configured to allow either MD5 or 96-bit MAC algorithms, both of which are considered weak.  Note that this plugin only checks for the options of the SSH server, and it does not check for vulnerable software versions. | |
| **Recommendations** | |
| Contact the vendor or consult product documentation to disable MD5 and 96-bit MAC algorithms. | |

**57. SSLv3 Padding Oracle On Downgraded Legacy Encryption Vulnerability (POODLE)**

|  |  |
| --- | --- |
| **Risk** | **Low** |
| **Affected Hosts** | **192.168.60.131:5432, 192.168.60.131:25** |
| **References** | **CVE-2014-3566** |
| **Description** | |
| The remote host is affected by a man-in-the-middle (MitM) information disclosure vulnerability known as POODLE. The vulnerability is due to the way SSL 3.0 handles padding bytes when decrypting messages encrypted using block ciphers in cipher block chaining (CBC) mode. MitM attackers can decrypt a selected byte of a cipher text in as few as 256 tries if they are able to force a victim application to repeatedly send the same data over newly created SSL 3.0 connections.  As long as a client and service both support SSLv3, a connection can be 'rolled back' to SSLv3, even if TLSv1 or newer is supported by the client and service.  The TLS Fallback SCSV mechanism prevents 'version rollback' attacks without impacting legacy clients; however, it can only protect connections when the client and service support the mechanism. Sites that cannot disable SSLv3 immediately should enable this mechanism.  This is a vulnerability in the SSLv3 specification, not in any particular SSL implementation. Disabling SSLv3 is the only way to completely mitigate the vulnerability. | |
| **Recommendations** | |
| Disable SSLv3.  Services that must support SSLv3 should enable the TLS Fallback SCSV mechanism until SSLv3 can be disabled. | |

**58. SSL/TLS EXPORT\_DHE <= 512-bit Export Cipher Suites Supported (Logjam)**

|  |  |
| --- | --- |
| **Risk** | **Low** |
| **Affected Hosts** | **192.168.60.131:25** |
| **References** | **CVE-2015-4000** |
| **Description** | |
| The remote host supports EXPORT\_DHE cipher suites with keys less than or equal to 512 bits. Through cryptanalysis, a third party can find the shared secret in a short amount of time.  A man-in-the middle attacker may be able to downgrade the session to use EXPORT\_DHE cipher suites. Thus, it is recommended to remove support for weak cipher suites. | |
| **Recommendations** | |
| Reconfigure the service to remove support for EXPORT\_DHE cipher suites. | |

**59. SSL/TLS Diffie-Hellman Modulus <= 1024 Bits (Logjam)**

|  |  |
| --- | --- |
| **Risk** | **Low** |
| **Affected Hosts** | **192.168.60.131:25** |
| **References** | **CVE-2015-4000** |
| **Description** | |
| The remote host allows SSL/TLS connections with one or more Diffie-Hellman moduli less than or equal to 1024 bits. Through cryptanalysis, a third party may be able to find the shared secret in a short amount of time (depending on modulus size and attacker resources). This may allow an attacker to recover the plaintext or potentially violate the integrity of connections. | |
| **Recommendations** | |
| Reconfigure the service to use a unique Diffie-Hellman moduli of 2048 bits or greater. | |

**60. SSH Weak Key Exchange Algorithms Enabled**

|  |  |
| --- | --- |
| **Risk** | **Low** |
| **Affected Hosts** | **192.168.60.131:22** |
| **References** | **n/a** |
| **Description** | |
| The remote SSH server is configured to allow key exchange algorithms which are considered weak.  This is based on the IETF draft document Key Exchange (KEX) Method Updates and Recommendations for Secure Shell (SSH) RFC9142. Section 4 lists guidance on key exchange algorithms that SHOULD NOT and MUST NOT be enabled. This includes:   diffie-hellman-group-exchange-sha1   diffie-hellman-group1-sha1   gss-gex-sha1-\*   gss-group1-sha1-\*   gss-group14-sha1-\*   rsa1024-sha1  Note that this plugin only checks for the options of the SSH server, and it does not check for vulnerable software versions. | |
| **Recommendations** | |
| Contact the vendor or consult product documentation to disable the weak algorithms. | |