Mitigation

OpenVAS critical vulnerabilities mitigation:

1. **Threat Level:** High
   CVSS: 10.0
   Port/Protocol: 8787/tcp
   NVT: Distributed Ruby (dRuby/DRb) Multiple Remote Code Execution Vulnerabilities
   Summary: Systems using Distributed Ruby (dRuby/DRb), which is available in Ruby versions 1.6 and later, may permit unauthorized systems to execute distributed commands.
   Solution type: Mitigation | Administrators of environments that rely on Distributed Ruby should ensure that appropriate controls are in place. Code-level controls may include: - Implementing taint on untrusted input - Setting $SAFE levels appropriately (>=2 is recommended if untrusted hosts are allowed to submit Ruby commands, and >=3 may be appropriate) - Including drb/acl.rb to set ACLEntry to restrict access to trusted hosts.
   Solution type: Mitigation | Implementing taint on untrusted input; Setting $SAFE levels appropriately (>=2 is recommended if untrusted hosts are allowed to submit Ruby commands, and >=3 may be appropriate); Including drb/acl.rb to set ACLEntry to restrict access to trusted hosts

2. **Threat Level:** High
   CVSS: 7.5
   Port/Protocol: 21/tcp
   NVT: vsftpd Compromised Source Packages Backdoor Vulnerability
   Summary: vsftpd is prone to a backdoor vulnerability.
   Solution type: VendorFix | The repaired package can be downloaded from the referenced link. Please validate the package with its signature.
   Link: https://security.appspot.com/vsftpd.html

3. **Threat Level:** High
   CVSS: 7.5
   Port/Protocol: 6200/tcp
   NVT: vsftpd Compromised Source Packages Backdoor Vulnerability
   Summary: vsftpd is prone to a backdoor vulnerability.
   Solution type: VendorFix | The repaired package can be downloaded from the referenced link. Please validate the package with its signature.
   Link: https://security.appspot.com/vsftpd.html

4. **Threat Level:** High
   CVSS: 9.3
   Port/Protocol: 3632/tcp
   NVT: DistCC Remote Code Execution Vulnerability

Summary: DistCC 2.x, as used in XCode 1.5 and others, when not configured to restrict access to the server port, allows remote attackers to execute arbitrary commands via compilation jobs, which are executed by the server without authorization checks.
Solution type: VendorFix | Vendor updates are available. Please see the references for more information. For more information about DistCC's security see the references.
Link: https://distcc.github.io/security.html

5. **Threat Level:** High
   CVSS: 9.0
   Port/Protocol: 5900/tcp
   NVT: VNC Brute Force Login
   Summary: It was possible to connect to the VNC server with the password: password
   Solution type: Mitigation | Change the password to something hard to guess or enable password protection at all.

6. **Threat Level:** High
   CVSS: 10.0
   Port/Protocol: 80/tcp
   NVT: TWiki XSS and Command Execution Vulnerabilities
   Summary: The host is running TWiki and is prone to Cross-Site Scripting (XSS) and Command Execution Vulnerabilities.
   Solution type: VendorFix | Upgrade to version 4.2.4 or later.

7. **Threat Level:** High
   CVSS: 7.5
   Port/Protocol: 80/tcp
   NVT: PHP-CGI-based setups vulnerability when parsing query string parameters from php files.
   Summary: Many PHP installation tutorials instruct the user to create a file called phpinfo.php or similar containing the phpinfo() statement. Such a file is often left back in the webserver directory.
   Solution type: Workaround | Delete the listed files or restrict access to them:
   http://192.168.1.154/mutillidae/phpinfo.php
   http://192.168.1.154/phpinfo.php

8. **Threat Level:** High
   CVSS: 7.5
   Port/Protocol: 80/tcp
   NVT: PHP-CGI-based setups vulnerability when parsing query string parameters from php files.
   Summary: PHP is prone to an information-disclosure vulnerability. Vulnerable url: http://192.168.1.154/cgi-bin/php. This may allow the attacker to obtain sensitive information and to run arbitrary PHP code on the affected computer.
   Solution type: VendorFix | PHP has released version 5.4.3 and 5.3.13 to address this vulnerability. PHP is recommending that users upgrade to the latest version of PHP.

9. **Threat Level:** High
   CVSS: 7.5
   Port/Protocol: 80/tcp
   NVT: Test HTTP dangerous methods.
   Summary: Enabled PUT/DELETE method: This might allow an attacker to upload and run arbitrary code on this web server.
   Solution type: Mitigation | Use access restrictions to these dangerous HTTP methods or disable them completely.

10. **Threat Level:** High
    CVSS: 10.0
    Port/Protocol: 80/tcp
    NVT: Possible Backdoor: Ingreslock.
    Summary: A backdoor is installed on the remote host.
    Solution type: Workaround| Enable firewall TCP 1524

11. **Threat Level:** High
    CVSS: 10.0
    Port/Protocol: 1099/tcp
    NVT: Java RMI Server Insecure Default Configuration Remote Code Execution Vulnerability.
    Summary: Multiple Java products that implement the RMI Server contain a vulnerability that could allow an unauthenticated, remote attacker to execute arbitrary code on a targeted system with elevated privileges.
    Solution type: Workaround| Disable class-loading.

12. **Threat Level:** High
    CVSS: 9.0
    Port/Protocol: 5432/tcp
    NVT: PostgreSQL weak password.
    Summary: It was possible to login into the remote PostgreSQL as user postgres using weak credentials.
    Solution type: Mitigation | Change the password as soon as possible.

13. **Threat Level:** High
    CVSS: 10.0
    Port/Protocol: 512/tcp
    NVT: rexec Passwordless / Unencrypted Cleartext Login.
    Summary: The rexec service is not allowing connections from this host.
    Solution type: Mitigation | Disable the rexec service and use alternatives like SSH instead.

14. **Threat Level:** High
    CVSS: 10.0
    Port/Protocol: High general/tcp
    NVT: OS End Of Life Detection.

Summary: The Operating System on the remote host has reached the end of life and should not be used anymore.
Solution type: Mitigation | Upgrade to a supported version of operating system.

15. **Threat Level:** High
CVSS: 10.0
Port/Protocol: High general/tcp
NVT: OS End Of Life Detection.
Summary: The Operating System on the remote host has reached the end of life and should not be used anymore.
Solution type: Mitigation | Upgrade to a supported version of operating system.

Nessus critical vulnerabilities mitigation:

1. **Threat Level:** Critical
CVSS: 9.8
Port/Protocol: 1524/tcp
Vulnerability: 51988 - Bind Shell Backdoor Detection.
Summary: 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.
Solution type: Mitigation | Require escalated user privileges to access the shell.

2. **Threat Level:** Critical
CVSS: 8.3
Port/Protocol: 22/tcp
Vulnerability: 32314 - Debian OpenSSH/OpenSSL Package Random Number Generator Weakness.
Summary: 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.
Solution type: Mitigation | Generate secure ssh keys with a stronger algorithm.

3. **Threat Level:** Critical
CVSS: 8.3
Port/Protocol: 5432/tcp
Vulnerability: 32321 - Debian OpenSSH/OpenSSL Package Random Number Generator Weakness (SSL check).
Summary: The remote SSL certificate uses a weak key.
Solution type: Mitigation | Generate secure ssh keys with a stronger algorithm to enforce a stronger certificate.

4. **Threat Level:** Critical
CVSS: 10.0
Port/Protocol: 2049/udp
Vulnerability: 11356 - NFS Exported Share Information Disclosure.

Summary: 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.
Solution type: Mitigation | Configure NFS on the remote host so that only authorized hosts can mount its remote shares.

5. **Threat Level:** Critical
   CVSS: 10.0
   Port/Protocol: 0/tcp
   Vulnerability: 33850 - Unix Operating System Unsupported Version Detection.
   Summary: The operating system running on the remote host is no longer supported.
   Solution type: Mitigation | Upgrade to a supported version of operating system.

6. **Threat Level:** Critical
   CVSS: 10.0
   Port/Protocol: 5900/tcp
   Vulnerability: 61708 - VNC Server 'password' Password.
   Summary: The operating system running on the remote host is no longer supported.
   Solution type: Mitigation | Secure the VNC service with a strong password.