Mitigations for 10.10.148.71

1. High-Severity Vulnerabilities

Vulnerability Name (OpenVAS NVT)	CVSS	Simple, Actionable Fixes/Mitigations
Microsoft Windows SMB Server Multiple Vulnerabilities-Remote (MS17-010)	**9.3 (High)**	* **Immediate Action: Patching is Critical.** This vulnerability (known as EternalBlue) allows for remote code execution and was used in major global ransomware attacks (WannaCry, NotPetya). **Patching is mandatory.** [1] * **Primary Fix (VendorFix):** Run **Windows Update** immediately. Ensure that the specific Security Update **MS17-010** (for supported OS versions) or the relevant Cumulative Update is installed. For older, unsupported operating systems (like Windows XP/Vista/Server 2003), Microsoft did release an out-of-band patch, which must be manually applied. [2] * **Mitigation (if immediate patch fails):** Disable the **Server Message Block Version 1 (SMBv1)** protocol entirely, as the flaw exists in this legacy protocol. This is highly recommended even after patching. * **Mitigation Steps (Windows PowerShell or Command Prompt): Disable SMBv1:** Disable-WindowsOptionalFeature -Online -FeatureName SMB1Protocol **OR** sc.exe config lanmanserver depend= bowser/mrxsmb20/mrxsmb30 & sc.exe config mrxsmb10 start= disabled * **Block External Access:** Use a firewall to **block TCP ports 139 and 445** from external (Internet) access. These ports are only needed for local network file sharing. [3]

2. Medium-Severity Vulnerabilities

Vulnerability Name (OpenVAS NVT)	CVSS	Simple, Actionable Fixes/Mitigations
DCE/RPC and MSRPC Services Enumeration Reporting	**5.0 (Medium)**	* **Vulnerability Insight:** This is an informational finding, as the exposure of services is inherent to how Windows functions on a network. The impact is providing an attacker with more intelligence (reconnaissance). [4] * **Mitigation (Firewalling):** The most effective mitigation is to use a **host-based firewall (Windows Firewall)** to filter incoming traffic to the exposed dynamic ports (49152, 49153, etc.) and the static mapping port **TCP 135**. * **Rule:** Create an inbound rule to **deny access to TCP 135** (and the associated dynamic ports) from any subnet that doesn't strictly require RPC/MSRPC communication (i.e., filter down to only trusted internal network segments). [5]
SSL/TLS: Report Weak Cipher Suites	**4.3 (Medium)**	* **Immediate Action: Disable RC4 Ciphers.** The detected ciphers (TLS_RSA_WITH_RC4_128_MD5 and TLS_RSA_WITH_RC4_128_SHA) use the **RC4** algorithm, which is considered cryptographically weak and subject to attacks. [6] * **Primary Fix (Configuration Change):** Modify the SSL/TLS configuration for the service running on port **3389/tcp (likely RDP)** to **disable TLS 1.0** entirely and remove all weak cipher suites. * **Windows Registry Fix:** Use the **Local Group Policy Editor (gpedit.msc)** or directly edit the Windows Registry under HKEY_LOCAL_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\Schannel\Ciphers and ...Protocols to ensure only strong ciphers (e.g., those using AES-256 or ChaCha20) and modern protocols (TLS 1.2/1.3) are enabled. * **Tool-Assisted Configuration:** Use tools like **IIS Crypto** (if the service is IIS-based) or a reliable PowerShell script to easily manage and apply secure cipher suite configurations to the system. [7]
SSL/TLS: Certificate Signed Using A Weak	**4.0 (Medium)**	* **Primary Fix (Certificate Replacement):** The certificate (CN=Jon-PC) is signed with the **SHA-1 hashing algorithm**, which is cryptographically weak. You must **obtain and install a**

Vulnerability Name (OpenVAS NVT)	CVSS	Simple, Actionable Fixes/Mitigations
Signature Algorithm (SHA-1)		**new certificate** from a Certificate Authority (CA) that uses a strong algorithm like **SHA-256 (SHA-2)** or newer. [8] * **Affected Service:** This likely affects the **Remote Desktop Protocol (RDP)** service running on **3389/tcp**. * **Mitigation:** While waiting for the new certificate, ensure that all connections to the service are only accepted from known, trusted clients and networks (using firewall rules or VPNs) to limit exposure to man-in-the-middle attacks. [9]

3. Low-Severity Vulnerabilities

Vulnerability Name (OpenVAS NVT)	CVSS	Simple, Actionable Fixes/Mitigations
TCP timestamps	**2.6 (Low)**	* **Vulnerability Insight:** This is not a direct vulnerability, but an informational disclosure that allows an attacker to compute the host's uptime, which can aid in targeted attacks. [10] * **Mitigation (Windows):** For Windows systems, execute the following command in an elevated Command Prompt or PowerShell: **Disable Timestamps:** netsh int tcp set global timestamps=disabled * **Note:** As indicated in the report, Windows Server 2008/Vista and newer may not completely disable the timestamp option but will prevent the system from using them when initiating new connections. [11]

Mitigations for 192.168.1.98

1. High-Severity Vulnerabilities (CVSS 7.5 - 10.0)

Vulnerability Name (OpenVAS NVT)	CVSS	Simple, Actionable Fixes/Mitigations
OS End Of Life Detection (Ubuntu 8.04)	**10.0**	* **Primary Fix (Mandatory): IMMEDIATELY migrate or upgrade** the operating system to a currently supported **Long-Term Support (LTS) version of Ubuntu** (e.g., Ubuntu 22.04 LTS or newer). EOL operating systems are not patched, making every service a high-risk vulnerability. * **Mitigation (Temporary):** If immediate migration is impossible, **isolate the host** entirely from external networks and strictly limit access to only necessary administrative IPs within the internal network.
TWiki XSS and Command Execution	**10.0**	* **Primary Fix (VendorFix): Upgrade TWiki** from the highly outdated version (01.Feb.2003) to the **latest stable version (4.2.4 or later)**. * **Mitigation:** If immediate upgrade is impossible, **remove or disable the TWiki application** until it can be patched, as this flaw allows for **remote code execution**.
DistCC Remote Code Execution	**9.3**	* **Primary Fix (VendorFix/Mitigation):** Since the id command executed successfully, the system is wide open. You must: 1. **Uninstall DistCC** if it is not absolutely needed. 2. If DistCC is necessary, **restrict network access** to the daemon by configuring the **allowed IP list** in the /etc/default/distcc file (or equivalent) to only include trusted clients. Block TCP port **3632** at the host firewall level for all untrusted IPs.
MySQL / MariaDB weak password	**9.0**	* **Primary Fix (Mitigation): Change the default 'root' password** immediately using a strong, unique, and complex password. **Command:** mysql -u root -p then ALTER USER 'root'@'localhost' IDENTIFIED BY 'YourStrongNewPassword!'; (or equivalent command for your MySQL version). * **Enhancement:** Configure the **MySQL database** to only listen on the **loopback address (127.0.0.1)** by changing the bind-address setting in the configuration file (/etc/mysql/my.cnf or equivalent). Block port **3306** at the firewall.
PostgreSQL weak password	**9.0**	* **Primary Fix (Mitigation): Change the default 'postgres' password** immediately. * **Command (Linux):** sudo -u postgres psql then \password postgres to set a strong, unique password. *

Vulnerability Name (OpenVAS NVT)	CVSS	Simple, Actionable Fixes/Mitigations
		Enhancement: Configure **PostgreSQL** to only listen on the **loopback address (127.0.0.1)** by setting listen_addresses = 'localhost' in postgresql.conf. Block port **5432** at the firewall.
SSH Brute Force Logins With Default Credentials	**7.5**	* **Primary Fix (Mitigation): Change the passwords** for the exposed accounts (msfadmin, user) immediately to strong, complex passwords. * **Best Practice: Disable password authentication** entirely for SSH and enforce the use of **SSH Keys** instead. * **Enhancement:** Disable root login, implement a strong **Fail2Ban** policy, and move the SSH service from default port **22/tcp** to a high, non-standard port.
phpinfo() output Reporting	**7.5**	* **Primary Fix (Workaround): Immediately delete the file** http://192.168.1.98/phpinfo.php and any similar file that exposes sensitive system and configuration details.
Apache httpd Range Header DoS	**7.8**	* **Primary Fix (Mitigation):** Apply the **Mitigation (Fix for CVE-2011-3192)** by limiting the number of headers or patching the Apache HTTP Server. * **Mitigation Steps (Apache config):** Add the directive LimitRequestFields 20 to your main configuration file to reduce the max number of request headers, which helps prevent this DoS attack. The best solution is a modern OS and a patched web server.
Tiki Wiki CMS Groupware < 4.2 Multiple Unspecified Vulnerabilities	**7.5**	* **Primary Fix (VendorFix): Upgrade the Tiki Wiki CMS Groupware** from the ancient version (1.9.5) to the **latest stable version** (or at least **4.2**). * **Mitigation:** Due to the severity (SQL Injection, Authentication Bypass), **take the application offline** until it is properly patched.

---

2. Medium-Severity Vulnerabilities (CVSS 4.3 - 6.8)

Vulnerability Name (OpenVAS NVT)	CVSS	Simple, Actionable Fixes/Mitigations
TWiki Cross-Site Request Forgery	**6.8, 6.0**	* **Primary Fix (VendorFix): Upgrade TWiki** to the latest stable version, which includes patches for both **4.3.1** and **4.3.2** (and later) to fix these CSRF vulnerabilities. * **Mitigation:** Ensure that user-authenticated sessions expire quickly.
Multiple Vendors STARTTLS Implementation Plaintext Arbitrary Command Injection	**6.8**	* **Primary Fix (VendorFix): Update the affected Mail Transfer Agent (MTA)** software (e.g., Postfix, Qmail, Sendmail, etc.) to the latest patched version. This is a severe flaw that can lead to command execution and password theft.
SSL/TLS: OpenSSL CCS Man in the Middle Security Bypass	**6.8**	* **Primary Fix (VendorFix): Update the OpenSSL library** on the Ubuntu host to a patched version (**0.9.8za, 1.0.0m, 1.0.1h, or later**). * **Command (Ubuntu):** sudo apt update && sudo apt upgrade openssl
Tiki Wiki CMS Groupware SQL Injection / File Inclusion / Input Sanitation	**6.5, 5.0, 5.0**	* **Primary Fix (VendorFix): Upgrade Tiki Wiki** to at least **version 17.2 or later** to resolve these multiple high-impact vulnerabilities.
HTTP Debugging Methods (TRACE/TRACK) Enabled	**5.8**	* **Primary Fix (Mitigation): Disable the TRACE method** in the Apache web server configuration to prevent Cross-Site Tracing (XST) attacks. * **Configuration Steps (Apache):** Add the directive TraceEnable Off to your Apache configuration file (httpd.conf or equivalent).
Cleartext Transmission of Sensitive Information via HTTP	**4.8**	* **Primary Fix (Workaround): Enforce the use of HTTPS (SSL/TLS)** for the web application (TWiki). * **Configuration Steps:** 1. Obtain and install a valid SSL certificate. 2. Configure the web server (Apache) to **redirect all HTTP traffic on port 80 to HTTPS on port 443**. This prevents cleartext passwords from being transmitted.
Telnet Unencrypted Cleartext Login	**4.8**	* **Primary Fix (Mitigation): Disable the Telnet service** entirely, as it transmits credentials in plain text. * **Best**

Vulnerability Name (OpenVAS NVT)	CVSS	Simple, Actionable Fixes/Mitigations
		Practice: Replace Telnet with SSH for all remote administrative access. SSH provides an encrypted channel.
SSL/TLS: Certificate Expired (25/tcp, 5432/tcp)	**5.0**	* **Primary Fix (Mitigation): Replace the expired SSL/TLS certificates** used by the Mailserver (Port 25) and PostgreSQL (Port 5432) with new, valid certificates. Expired certificates break trust and often cause application errors.
Check if Mailserver answer to VRFY and EXPN requests	**5.0**	* **Primary Fix (Workaround): Disable the VRFY and EXPN commands** in the Mailserver configuration (Postfix/Sendmail). These commands disclose valid user account names, which helps attackers harvest targets for brute-force attacks. * **Configuration (Postfix):** Add disable_vrfy_command = yes to the main.cf configuration file.
SSL/TLS: 'DHE_EXPORT' Man in the Middle Security Bypass (LogJam)	**4.3**	* **Primary Fix (VendorFix): Remove support for DHE_EXPORT cipher suites** from the service (Mailserver on Port 25) and **update OpenSSL** to a patched version to protect against the LogJam vulnerability.