**Review and Document Critical Vulnerabilities**

I have identified:

* **SSL Certificate Cannot Be Trusted** (Plugin #51192)
* **SMB Signing Not Required** (Plugin #57608).

**Mitigation Steps**

1. **SSL Certificate Cannot Be Trusted**
   * **Issue**: The server uses an invalid, expired, or untrusted SSL certificate.
   * **Fix**: Obtain a valid SSL certificate from a trusted Certificate Authority (CA), update the server's certificate, and configure the web server to use it.
2. **SMB Signing Not Required**
   * **Issue**: SMB signing is not enforced, which can allow man-in-the-middle attacks.
   * **Fix**: Configure the host/server to enforce SMB message signing. On Windows, enable the **"Microsoft network server: Digitally sign communications (always)"** policy.