



Vulnerability Name: SMB Signing not required

Severity: Medium

CVE ID: 57608

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.

Suggested Fix : 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.

Vulnerability Name: SSL Certificate Cannot Be Trusted

Severity : Medium

CVE ID : 51192

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.

 $\label{thm:suggested} \mbox{Suggested Fix} \quad : \mbox{Purchase or generate a proper SSL certificate for this service}.$

Those two were the major vulnarabilities found