GUIDE
SMB Protocol: Function and Security Risks

v1.0.0

Author:

Eldon Gabriel

August 24, 2025

TABLE OF CONTENTS

REVISION HISTORY

Version	Date	Author	Description of Changes
v1.0.0	08/24/2025	Eldon G.	Initial draft.

EXECUTIVE SUMMARY

This report reviews the SMB protocol, which allows computers to connect over a network and share files, printers, and other resources. SMB is commonly used in organizations to help employees work together and manage tasks more efficiently. The report outlines how SMB works, its different versions, and common uses in Windows networks, including Active Directory and centralized access management.

It also highlights security risks, particularly with SMBv1, which is outdated and vulnerable to attacks like EternalBlue and WannaCry. The report recommends disabling SMBv1, keeping systems up to date, limiting exposure to public networks, applying firewalls, and using network segmentation. Combined with regular audits and staff training, these measures create a strong, multi-layered defense against SMB-related threats.

Disclaimer: This guide is based on independent research and understanding of SMB protocol and security practices. It does not include proprietary lab solutions from MCSI.

1.0 INTRODUCTION

1.1 Project Overview

Server Message Block (SMB) is a protocol that lets computers on a network share files, printers, and other resources with one another. It allows employees in a business to work together more easily by accessing shared resources quickly. SMB is used in many organizations because it makes communication and file management simpler across multiple systems.

However, SMB also has security risks. Its wide use and complex features make it a target for cyber attackers. Past vulnerabilities in SMB have caused major security incidents, such as the WannaCry ransomware attack. Businesses need to balance SMB's convenience with strong security practices. Regular updates, correct configuration, and network separation are important to reduce risks while still using SMB effectively.

2.0 HOW SMB WORKS

2.1 Protocol Operation

SMB works on a client-server model. The client computer asks for access to files, printers, or other resources, and the server computer responds with the requested data or service. This setup allows multiple users to access shared resources on the network efficiently.

2.2 Protocol Versions

SMB has gone through several versions, each adding better performance, security, and features:

- **SMB 1.0** – The first version, now outdated and not secure.
- **SMB 2.0** – Offers faster performance and reduces network traffic.
- **SMB 3.0** – Adds encryption, multichannel connections for faster data transfer, and better protection against attacks like man-in-the-middle.

Using older versions like SMB 1.0 is not recommended because they can make networks unsafe. SMB usually communicates through TCP ports 139 and 445. Port 139 works with NetBIOS over TCP/IP, while port 445 lets computers communicate directly without using NetBIOS. The client connects to the server on these ports and sends requests, which the server responds to for file or printer access.

3.0 COMMON USES IN THE REAL WORLD

In Windows networks, SMB is used for file and printer sharing. It lets employees access files across multiple computers. Windows domains use centralized authentication, which lets administrators manage who can access different resources based on user permissions.

Sharing files and printers improves collaboration in offices. Employees can work on projects together, share documents, and use shared printers without extra setup. Active Directory makes this process even better by organizing users, computers, and resources in a structured way. It gives administrators detailed control over access, simplifies user management, and provides a single login for all services. SMB is essential for organizations looking to improve workflow and productivity.

4.0 SECURITY RISKS

Exploits like EternalBlue and the WannaCry ransomware show the dangers of vulnerable SMB systems. EternalBlue targeted a flaw in SMBv1, allowing attackers to run code on other computers. WannaCry used EternalBlue to spread across networks, encrypting files, and demanding ransom.

Because of these risks, SMBv1 is now deprecated. SMBv1 does not have modern security features and is open to attacks. Microsoft advises using SMBv2 or SMBv3 instead. To reduce risks, organizations should:

- Keep systems updated with security patches.
- Limit SMB exposure, especially to the internet.
- Turn off unneeded SMB services.
- Apply firewalls to control SMB traffic to trusted networks only.

Defensive Measures

Disabling SMBv1 is critical. This outdated version is easy for attackers to exploit. Organizations should check that all systems work with SMBv2 or SMBv3 before disabling SMBv1.

Blocking SMB from public networks, using firewalls, and segmenting networks also improve security. Firewalls filter and monitor SMB traffic, while segmentation isolates sensitive systems to prevent malware from spreading. These steps together create strong, multi-layered protection.

5.0 CONCLUSION

Turning off SMBv1 is essential for modern network security. SMBv1 is updated and lacks encryption, making it risky. Organizations should check that all devices support SMBv2 or SMBv3 before removing SMBv1.

Blocking SMB from public networks prevents attackers from accessing the network. Firewalls and network segmentation add more protection by controlling traffic and isolating critical systems.

Regular security audits and employee training also help. Staff should understand SMB risks and follow safe file-sharing practices. Using these measures together creates a strong defense, reduces risks, and helps organizations stay secure against evolving cyber threats.