SMB Security Best Practices | CISA

Published: 2017-03-16 · Archived: 2026-04-06 01:58:13 UTC

In response to public reporting of a potential Server Message Block (SMB) vulnerability, US-CERT is providing known best practices related to SMB. This service is universally available for Windows systems, and legacy versions of SMB protocols could allow a remote attacker to obtain sensitive information from affected systems.

US-CERT recommends that users and administrators consider:

- disabling SMBv1 and
- blocking all versions of SMB at the network boundary by blocking TCP port 445 with related protocols on UDP ports 137-138 and TCP port 139, for all boundary devices.

US-CERT cautions users and administrators that disabling or blocking SMB may create problems by obstructing access to shared files, data, or devices. The benefits of mitigation should be weighed against potential disruptions to users. For more information on SMB, please review Microsoft Security Advisories 2696547 and 204279.
