Government of India
National Critical Information Infrastructure Protection Centre
(A Unit of NTRO)

Date: 13 Nov 2019

Cyber Security Advisory: SMB Protocol (445/TCP)

The SMB (Server Message Block) is mostly used for local network file sharing and access to remote services in many organization who use Windows PCs in their environment. SMB is also a really good example of low-hanging fruit for attackers, because it's a protocol used across many services and has a lengthy history of insecure configurations or implementation bugs. For threat actors, this means they can easily gain access to a server using the SMB protocol and then pivot from that server into other services and applications across the organization. Since many organizations still rely on SMB, new exploits, threats, and breaches related to the protocol are published regularly.

MalwareBytes Labs indicated that, at the end of last year, two well-known malware attacks, Emotet and Trickbot, were tied to SMB vulnerabilities. As attackers gain access through SMB servers, they utilize worm-like functionality in both malware attacks to slowly propagate through the organization.

Steps to secure SMB:

Users and administrators may 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.

Reference: https://www.us-cert.gov/ncas/current-activity/2017/01/16/SMB-Security-Best-Practices

Disclaimer:

The information provided by NCIIPC above is on "as is" basis only. System owners are advised to independently evaluate the contents for its applicability in their specific environment, and take appropriate action as per their own assessment of the implications of the alert/ advisory on their systems. NCIIPC will not be liable for any issues or problems that may arise from application or non-application of the alert/ advisory. System owners are wholly responsible for cyber security updates to their information technology systems.

With Best Regards,
Knowledge Management System
National Critical Information Infrastructure Protection Centre
Block-III, Old JNU Campus, New Delhi - 110067
Website: www.nciipc.gov.in
Toll Free: 1800-11-4430