SMBv3 Vulnerabilities Explained

blog.netwrix.com/smbv3-vulnerability

Kevin Joyce

Workplaces have evolved. While hybrid and remote work existed before COVID-19, these working arrangements became even more prevalent during and after the pandemic. Today, workplaces offer the flexibility for employees to work and access company resources from anywhere worldwide, with the Server Message Block (SMB) protocol at the center of this. However, this flexibility has opened the door to more significant cyber security challenges because more than the traditional perimeter-based security model is required.

This article will explore these cyber security concerns, particularly in the SMBv3, and provide practical measures for identifying and mitigating them.

What is SMBv3?

Server Message Block (SMB) refers to a network protocol that allows applications, computers, and devices to communicate and share resources, such as files, printers, and serial ports, over a network. It facilitates communication between clients (devices requesting access to resources) and servers (devices providing resources) on a local area network (LAN) or across the internet.

Since its creation in the 1980s, SMB has had several iterations (with enhancements in performance and security), with SMBv3 being the latest one.

SMBv3 Vulnerabilities

Despite the major improvements made on SMBv3, it still presents some security vulnerabilities, with remote code execution being one of the most concerning. Remote code execution (RCE) is a security vulnerability that allows threat actors to execute or run malicious code on a computer or network, usually remotely, to gain complete control.

SMBGhost (CVE-2020-0796)

On March 10, 2020, Microsoft accidentally published information about a newly identified vulnerability (CVE-2020-0796) in SMBv3. While Microsoft quickly deleted this information, researchers had already noted it. This forced Microsoft to publish a formal advisory two days later (March 12, 2020).

These events led the security community to dub CVE-2020-0796 SMBGhost. According to Microsoft, this vulnerability could lead to remote code execution on the server, which is always a significant concern as a severe vulnerability.

Microsoft’s advisory highlighted that malicious actors can exploit this vulnerability by sending a specially crafted packet to a target, the SMBv3 server. This is highly similar to the SMBv1 vulnerability. The scary part about this vulnerability is that researchers deemed it “wormable,’’ which means if someone were to exploit one of your machines, it could potentially spread from machine to machine throughout your environment.

The version specifically affected was 3.1.1, the most recent version of SMBv3. Microsoft also listed that the vulnerability affected all Windows 10 and Windows Server running versions 1903 and 1909.

Fortunately, there are some potential mitigations and workarounds to avoid this issue, and as of 3/12/2020, Microsoft released a patch that addresses this vulnerability.

Handpicked related content:
[Free Guide] Ransomware Prevention Best Practices

CVE-2022-24508

Two years after the SMBGhost, on Mar 8, 2022, Microsoft released another security update relating to SMBv3. Described as a Win32 file enumeration remote code execution vulnerability, CVE-2022-24508 was another RCE vulnerability mainly affecting Windows 10 version 2004 and newer versions supporting SMBv3.

While there isn’t as much information about CVE-2022-24508 as on SMBGhost, it’s worth noting that Microsoft assigned the severity of this vulnerability as “important.” This means that organizations should still give it the attention it requires by taking steps to prevent it.

Risks and Impact of SMBv3 Vulnerabilities

Since the most significant security vulnerability of SMBv3 is RCE, this section will explore the risks related to this threat. These include the following:

- **Unauthorized Access:** The very first impact of an RCE attack is malicious actors gaining unauthorized access to an organization’s internal network. This can have serious consequences, like privilege escalation, which gives attackers more authority within the network to carry out more harmful actions.
- **Data Breaches:** Data, especially internal company data (company secrets), is one of the organizations’ most important assets. If this data were to fall into the wrong hands, it would have devastating effects. As such, one of the main reasons attackers carry out RCE attacks is to steal sensitive company data.
- **Propagation of Malware:** Once inside a network, attackers can spread malicious code through privilege escalation to other connected networks and devices.
- **Ransomware Attacks:** Threat actors can also use RCE attacks to hold company resources “hostage.” In such a situation, attackers lock out company administrators from the affected network or encrypt essential data and require payment in exchange for access.

- **Regulatory Non-Compliance:** Data breaches put your organization at risk of non-compliance with laws and regulations that govern data handling, such as the General Data Protection Regulation (GDPR) and the Health Insurance Portability and Accountability Act (HIPAA). This can lead to hefty fines from these regulators and a loss of customer trust.
- **Financial Losses:** Individually or combined, the risks discussed above can cause significant losses to affected organizations. Companies risk severe financial losses from paying ransoms to recovering from losses due to downtimes and paying fines due to regulatory compliance.

Prevention and Mitigation of SMBv3 Vulnerabilities

The first (and most obvious) step to prevent SMBv3 vulnerabilities is to apply the patches that Microsoft has provided in the past. This is the most effective way to mitigate identified vulnerabilities that have known solutions.

If, for whatever reason, you're not able to apply the patches in the short term, Microsoft has identified a workaround to prevent threat actors from exploiting it. The issue lies in SMB compression, so turning off this feature of SMB will protect you from an attacker attempting to exploit it.

```
Set-ItemProperty -Path "HKLM:
SYSTEMCurrentControlSetServicesLanmanServerParameters" DisableCompression -Type
DWORD -Value 1 -Force
```

The above PowerShell code will update your registry and turn off the compression feature on SMB servers. This will not protect your SMB clients; the code needed to update your clients is below:

```
Set-ItemProperty -Path "HKLM:
SYSTEMCurrentControlSetServicesLanmanServerParameters" DisableCompression -Type
DWORD -Value 0 -Force
```

Fortunately, neither of these updates to the registry requires a reboot to take effect.

One question you may have is about the impact turning off SMB compression will have. Microsoft mentions in their advisory that SMB compression isn't even used in Windows or Windows Server yet. It will have no negative performance impact.

Best Practices for Mitigating Risks Associated with SMBv3 Vulnerabilities

While applying the patches is essential and can help protect against SMBv2 vulnerabilities, there are several things you can do to ensure maximum protection of your organization's networks, including the following.

Use the Latest Versions of SMB

The latest versions of SMB will usually have updates that can help secure your network. As mentioned earlier, Microsoft has released several updates for SMB since it was first created. While the latest version is SMBv3, there have still been mini-updates within the version, and as of the writing of this article, the most recent one is SMB 3.1.1, built for Windows 10 and Windows Server 2016. For instance, this version has several updates that make it more secure than previous versions, such as:

- Encryption
- Directory caching
- Pre-authentication integrity
- Rolling cluster upgrade support

Segment Your Network

In case of an attack, threat actors can use privilege escalation to spread out the impact across connected networks. You can reduce the magnitude and scope of the attack by dividing your network into smaller, isolated segments or subnetworks. This way, even if hackers exploit a vulnerability in one segment, they can't use it to access another in your network.

Handpicked related content:

[Free Report] CyberEdge 2024 Cyberthreat Defense Report

Monitoring Network Traffic

Even with patches and implementing security best practices, you must be on the lookout for suspicious or abnormal behavior and even known attack signatures within your network. To do so, you can implement the following strategies:

- Establish a baseline of normal network behavior; any deviation from this should be flagged as a potential threat.
- Utilize Intrusion Detection Systems (IDS) and Intrusion Prevention Systems (IPS)
- Use network traffic analysis tools
- Analyze endpoint telemetry data and behavior patterns
- Enable logging on network devices

Configure Firewalls

Firewalls can be extremely helpful in protecting your network's integrity. They work by enforcing a deny policy, where your network blocks any incoming and outbound traffic that doesn't fall into the "allowed" category of the firewall's settings. For instance, if you configure firewalls to limit SMB traffic to specific IP addresses or subnets, you can help prevent unauthorized access from remote execution attacks.

How Netwrix Can Help

SMB vulnerabilities have been and always will be there. But just because this is the reality doesn’t mean you should accept this as the status quo and do nothing about it. You can and should take proactive measures to protect your organization’s network against security vulnerabilities and the associated risks.

Fortunately, Netwrix can help. We have Identity Threat Detection and Response (ITDR) solutions that can give you peace of mind. Netwrix ITDR solutions help you identify potential threats by providing real-time alerts. Once identified, these solutions help you quickly and automatically shut down the threats with pre-set playbooks. Finally, Netwrix facilitates a quick recovery process for your network by restoring it to its pre-attack state.

Need a proactive solution to prevent SMBv3 vulnerabilities? Contact us today to find out how we can help.

Kevin Joyce
Senior Technical Product Manager at Netwrix. Kevin is passionate about cyber-security and holds a Bachelor of Science degree in Digital Forensics from Bloomsburg University of Pennsylvania.