SMB Vulnerabilities in Healthcare

11/05/2020

The Wall of Constantinople

Mehmed II 27 foot Bronze Cannons

VS

Your Network
with SMBv1 Protocol

EternalBlue

- SMB Overview

- SMB Vulnerabilities

- SMB Exploitation and its Effects

- SMB and Healthcare

- SMB Identification Methods

- SMB Remediation

- Summary

- References

Slides Key:

Non-Technical: Managerial, strategic and high-level (general audience)

Technical: Tactical / IOCs; requiring in-depth knowledge (sysadmins, IRT)

Server Message Block (SMB)

is an enhanced version of CIFS (Common Internet File System) done by Microsoft for the release of Windows 95 in the early 1990s. Due to CIFS challenges with security, slow file transfer, and taking a lot of time responding to service requests and responses, SMB was developed.

Image source: Educba

SMB request, response

SMB is a client-server interaction protocol where clients request a file and the server provides it to the client. SMB gives users the ability to create, modify and delete shared files, folders, and printer access within the network.

SMB REQUESTS

SMB RESPONSES

Client

Server

- Printers
- Scanners
- File system
- Serial Port

PORT 445 ⟺ PORT 139

SMB runs directly over TCP (port 445) or over NetBIOS (usually port 139, rarely port 137 or 138).

SMB Versions

1984   **SMBv1.0**: Very similar to the CIFS protocol that shares the files over a network to access them among the clients in an effective way. SMB was initially introduced to run on top of NetBIOS and TCP/IP interface. *Version is the most vulnerable.

2006   **SMBv2.0**: Reduced the "chattiness" of SMB1.0 by lessening the number of commands and subcommands used to communicate. SMBv2 helped to store larger file data and communicate the large files over the network in less time.

2008   **SMBv2.1:** Introduced with Windows 7 and Server 2008 R2; introduced further performance enhancements with a new opportunistic locking mechanism.

2012   **SMBv3.0**: Introduced in WINDOWS 8 Server and windows server 2012. It was introduced to improve the encryption level end to end. It is sometimes called version 2.2.

2020   **SMBv3.1.1:** Introduced with Windows 10 Server and Windows server 2016. SMB 3.1.1 version uses the AES encryption algorithm to implement pre-authenticated security checks using the SHA-512 hash key. *Most up to date version.

Image source: Allot.com

Shodan search for "SMB version: 1" port: "445" OS: Windows
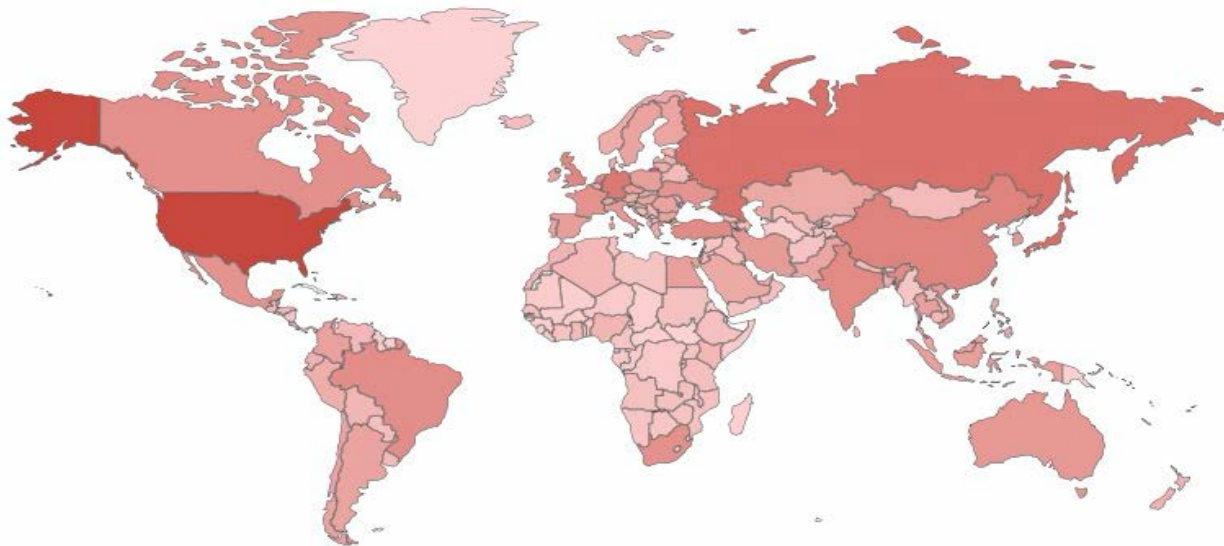
Top Countries	Hosts
United States	270,536
Russia	51,796
Hong Kong	51,351
Germany	48,741
Japan	44,064

The Shadow Brokers (hacker group) leaked a developed SMB exploit, also known as EternalBlue. Microsoft was forced to issue a critical security bulletin (MS17-010) on March 14, 2017. EternalBlue was used as the initial compromise vector or as a method of lateral movement for other cyberattacks such as WannaCry, Emotet, NotPetya and TrickBot.

Other related exploits labelled:
- ➢ Eternalromance
- ➢ Eternalchampion
- ➢ Eternalsynergy
- ➢ Eternalrocks

SMB RELATED CVE

Year	SMB RELATED CVE
2017	35
2018	29
2019	20
2020	6
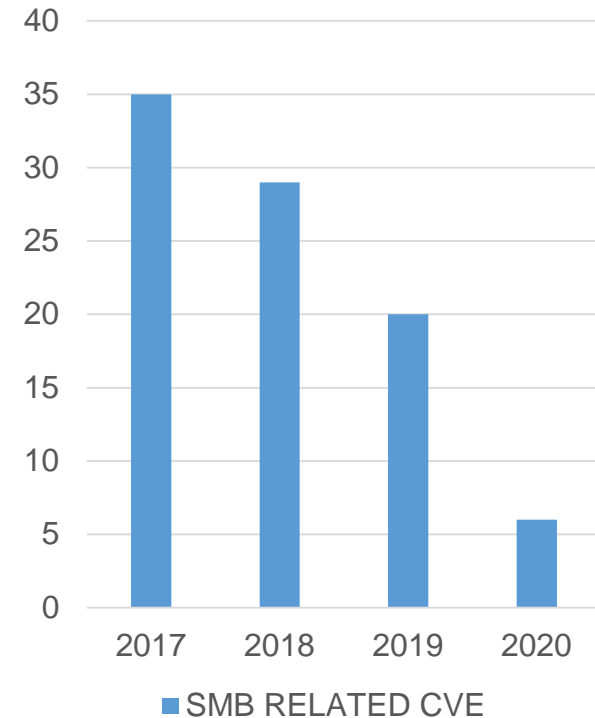
WannaCry	Takes advantage of SMBv1 vulnerability to compromise Windows machines, load malware, and propagate to other machines in a network.
Emotet	Emotet infections are initiated by different mailspam campaigns. Once Emotet is downloaded it can undetectably install Trickbot via SMB vulnerability onto the host system.
TrickBot	Uses standard attack vectors for infection to spread to other clients/servers such as malvertising, spear phishing, network vulnerabilities (SMB and RDP), and secondary payloads.
NotPetya	Malware that uses a variety of techniques to spread to other computers, including EternalBlue and EternalRomance. Known to target mostly Ukrainian industries.

EternalBlue	(SMBv1) server in various versions of Microsoft Windows mishandles specially crafted packets from remote attackers, allowing them to execute arbitrary code on the target computer.
EternalRomance	A RCE attack that exploits CVE-2017-0145 against the legacy SMBv1 file-sharing protocol.
EternalChampion	Triggers a race condition in how SMBv1 handles transactions. CVE-2017-0146
EternalSynergy	Proof of Concept (POC) that shows that incoming SMB messages are copied by an initial handler into the corresponding transaction buffer. CVE-2017-0146
EternalRocks	Uses seven NSA tools where WannaCry, for example, only used two (EternalBlue and another called DoublePulsar).

2017

Jan/Feb	March 12th	March 16th	April	May
Shadow Brokers leaks/warnings	MS17-010 released	CVE-2017-143 CVE-2017-144 CVE-2017-145 CVE-2017-146 CVE-2017-147 CVE-2017-148	Shadow Brokers release more exploits	WannaCry ransomware spreads worldwide

CVE-2017-143

The SMBv1 server affects:
- Microsoft Windows Vista SP2
- Windows Server 2008 SP2 and R2 SP1
- Windows 7 SP1
- Windows 8.1
- Windows Server 2012 Gold and R2
- Windows RT 8.1
- Windows 10 Gold, 1511, and 1607
- Windows Server 2016

This vulnerability allows remote attackers to execute arbitrary code via crafted packets.

This vulnerability is related to the following other vulnerabilities:

VULNERABILITY
CVE-2017-0144
CVE-2017-0145
CVE-2017-0146
CVE-2017-0147
CVE-2017-0148

MS17-010 once published initiated a series of additional vulnerabilities associated with SMBv1.

National Health Service (UK)

The WannaCry ransomware targeted computers running Microsoft Windows operating system by encrypting data and demanding ransom payment in the Bitcoin cryptocurrency. The initial infection was likely through an exposed vulnerable internet-facing SMB port according to the Lessons learned review of the WannaCry Ransomware Cyber Attack.

NHS

NHS Digital alerts Department of Health and Social Care at 13:00, 12 May

NHS England declared a major incident at 16:00 on 12 May

Kill switch discovered on the evening of 12 May: stopped further spread of malware

1,220
pieces of diagnostic equipment across the NHS were affected by WannaCry.

https://www.england.nhs.uk/wp-content/uploads/2018/02/lessons-learned-review-wannacry-ransomware-cyber-attack-cio-review.pdf

Healthcare Devices

The Clinical Information Center (CIC) Pro workstations are connected to CARESCAPE, a real-time monitoring network for medical facilities, so they can interact with and display data from other devices on the network, including telemetry servers and bedside monitors.

Image source: GE Healthcare

Processor Box

CVE-2020-6963 attackers have the ability to read and write access to all files on the system and affects CIC versions 4.x and 5.x, CSCS version 1.x, Apex Telemetry Server versions 4.2 and earlier, as well as CARESCAPE Telemetry Server versions 4.3 and earlier.

Ultrasound Products

Select Ultrasound products are affected by the Microsoft Windows SMBv1 vulnerabilities. The exploitability of the vulnerabilities depends on the actual configuration and deployment environment of each product.

Listens on network ports
139/tcp, 445/tcp or 3389/tcp.

Image source: Siemens Healthineers

LEADERSHIP FOR IT SECURITY & PRIVACY ACROSS HHS
HHS CYBERSECURITY PROGRAM
OFFICE OF INFORMATION SECURITY

DETECT
- PowerShell
- Registry Editor

ENABLE/DISBALE
- PowerShell
- Registry Editor
- Group Policy

AUDIT SMBv1 Usage
- PowerShell

Image source: NETFORT

```
Administrator: Windows PowerShell

Windows PowerShell
Copyright (C) 2016 Microsoft Corporation. All rights reserved.

PS C:\WINDOWS\system32> Get-SmbConnection

ServerName  ShareName  UserName                 Credential                Dialect NumOpens
----------  ---------  --------                 ----------                ------- --------
10.1.1.97   music      DARRAGH-LAPTOP\Darragh   DARRAGH-LAPTOP\Darragh    2.0.2   1
10.1.1.97   netfort    DARRAGH-LAPTOP\Darragh   DARRAGH-LAPTOP\Darragh    2.0.2   1
10.1.1.97   photos     DARRAGH-LAPTOP\Darragh   DARRAGH-LAPTOP\Darragh    2.0.2   1
10.1.1.97   shared     DARRAGH-LAPTOP\Darragh   DARRAGH-LAPTOP\Darragh    2.0.2   1
10.1.1.97   videos     DARRAGH-LAPTOP\Darragh   DARRAGH-LAPTOP\Darragh    2.0.2   1
```

Vulnerability Scanner

Various vulnerability scanners may help with this, but need to know which systems to query.
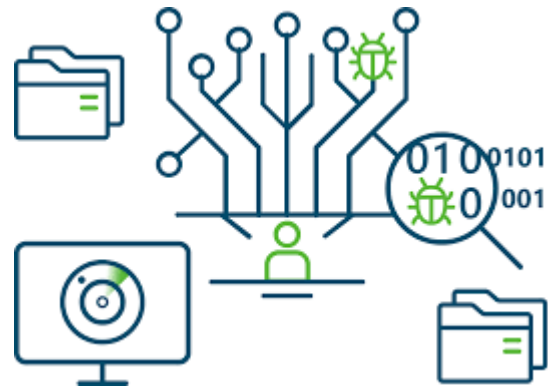
Network Tap

Capture network traffic by using a SPAN\Mirror port and detect version from a network traffic monitoring application.
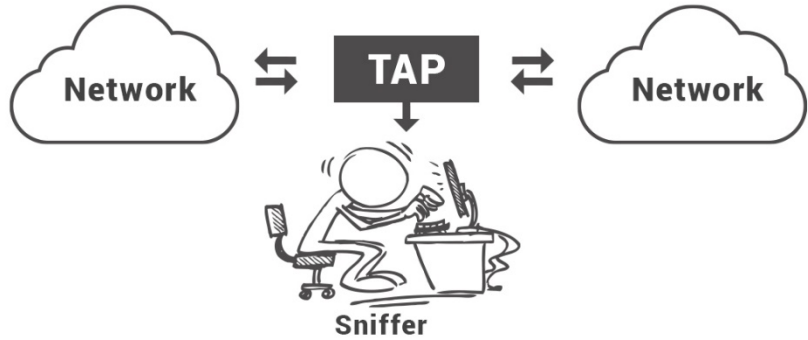
Image source: Leutert NetServices

LEADERSHIP FOR IT SECURITY & PRIVACY ACROSS HHS
HHS CYBERSECURITY PROGRAM
OFFICE OF INFORMATION SECURITY

Detect SMB Version/Dialect Negotiation Request through filters.

https://sharkfestus.wireshark.org/sharkfest.13/presentations/NAP-03_Microsoft-SMB-Troubleshooting_Rolf-Leutert.pdf

Image source: Wireshark Sharkfest

If certain features are enabled in the extraction of logs, SMB versions can be displayed through search.

Image source: Splunk Blog

Patch	Use recommended patches for specific systems and vulnerabilities.
Isolate and/or Replace	Disconnect the system(s) from network and use as standalone until patches can be administered.
Port Filter	Perimeter hardware and appliance firewalls that are positioned at the edge of the Network should block unsolicited communication from the known NETBIOS and SMB Ports 137-139 and 445.

Continue to do NOTHING =
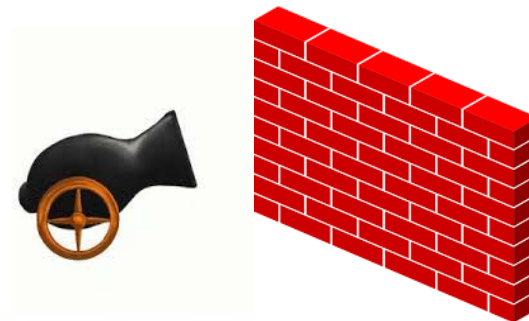
75% of unpatched vulnerabilities among SMBs are more than one year old, according to Alert Logic research. It's only a matter of time before there is another attack. As a recap, remember it only takes one determined attacker and one system to gain access to your wall or network. In order for Healthcare to prevent SMBv1 as the initial compromise vector or as a method of lateral movement for other cyber attacks, assessments and remediation's are needed. Let's be proactive!

Reference Materials

References

- How threat actors are using SMB vulnerabilities
  - https://blog.malwarebytes.com/101/2018/12/how-threat-actors-are-using-smb-vulnerabilities/

- Insecure configurations expose GE Healthcare devices to attacks
  - https://www.csoonline.com/article/3516093/insecure-configurations-expose-ge-healthcare-devices-to-attacks.html

- Eternalblue | The NSA-developed Exploit That Just Won't Die
  - https://www.sentinelone.com/blog/eternalblue-nsa-developed-exploit-just-wont-die/

- Security researcher creates new backdoor inspired by leaked NSA malware
  - https://www.zdnet.com/article/security-researcher-creates-new-backdoor-inspired-by-leaked-nsa-malware/

- SSA-701903: SMBv1 Vulnerabilities in Ultrasound Products from Siemens Healthineers
  - https://cert-portal.siemens.com/productcert/pdf/ssa-701903.pdf

- Hackers reportedly used a tool developed by the NSA to attack Baltimore's computer systems
  - https://www.theverge.com/2019/5/25/18639859/baltimore-city-computer-systems-cyberattack-nsa-eternalblue-wannacry-notpetya-cybersecurity

- CIFS VS SMB
  - https://www.educba.com/cifs-vs-smb/

- More Than Half of SMB Devices Run Outdated Operating Systems
  - https://www.darkreading.com/endpoint/more-than-half-of-smb-devices-run-outdated-operating-systems/d/d-id/1335142

- WannaCry Ransomware Using SMB Vulnerability
  - https://digital.nhs.uk/cyber-alerts/2017/cc-1411

- Lessons learned review of the WannaCry Ransomware Cyber Attack
  - https://www.england.nhs.uk/wp-content/uploads/2018/02/lessons-learned-review-wannacry-ransomware-cyber-attack-cio-review.pdf

- CIC Pro Clinical Information Center Service Manual
  - http://www3.gehealthcare.com/~/media/downloads/us/services/equipment%20services/support-center/daylight-savings-time/patient-monitoring/monitors/gehc-service-manual_cic-pro-clinical-info-center-mp100-v511-2011.pdf

- Finding and Fixing Vulnerabilities in SMB Shares Enumeration , a Medium Risk Vulnerability
  - https://beyondsecurity.com/scan-pentest-network-vulnerabilities-smb-shares-enumeration.html?cn-reloaded=1

- How to Determine Enabled SMB Versions
  - https://pattersonsupport.custhelp.com/app/answers/detail/a_id/39561/~/how-to-determine-enabled-smb-versions

- How to detect, enable and disable SMBv1, SMBv2, and SMBv3 in Windows
  - https://docs.microsoft.com/en-us/windows-server/storage/file-server/troubleshoot/detect-enable-and-disable-smbv1-v2-v3

- How to detect SMBv1 use on your Network
  - https://www.netfort.com/blog/detect-smbv1-use-network/

- [MS-CIFS]: Common Internet File System (CIFS) Protocol
  - https://docs.microsoft.com/en-us/openspecs/windows_protocols/ms-cifs/d416ff7c-c536-406e-a951-4f04b2fd1d2b?redirectedfrom=MSDN#published-version

- [MS-SMB2]: Server Message Block (SMB) Protocol Versions 2 and 3
  - https://docs.microsoft.com/en-us/openspecs/windows_protocols/ms-smb2/5606ad47-5ee0-437a-817e-70c366052962?redirectedfrom=MSDN

- CVE-2017-0143
  - https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-0143

- CVE-2017-0144
  - https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-0144

- CVE-2017-0145
  - https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-0145

- CVE-2017-0146
  - https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-0146

- CVE-2017-0147
  - https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-0147

- CVE-2017-0148
  - https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-0148

- NAP-3 Microsoft SMB Troubleshooting
  - https://sharkfestus.wireshark.org/sharkfest.13/presentations/NAP-03_Microsoft-SMB-Troubleshooting_Rolf-Leutert.pdf

- Petya ransomware and NotPetya malware: What you need to know now
  - https://www.csoonline.com/article/3233210/petya-ransomware-and-notpetya-malware-what-you-need-to-know-now.html

- SMB Exploited: WannaCry Use of "EternalBlue"
  - https://www.fireeye.com/blog/threat-research/2017/05/smb-exploited-wannacry-use-of-eternalblue.html

- NSA-leaking Shadow Brokers just dumped its most damaging release yet
  - https://arstechnica.com/information-technology/2017/04/nsa-leaking-shadow-brokers-just-dumped-its-most-damaging-release-yet/

- The Leaked NSA Spy Tool That Hacked the World
  - https://www.wired.com/story/eternalblue-leaked-nsa-spy-tool-hacked-world/

- Major Leak Suggests NSA Was Deep in Middle East Banking System
  - https://www.wired.com/2017/04/major-leak-suggests-nsa-deep-middle-east-banking-system/

- EternalBlue
  - https://www.cisecurity.org/wp-content/uploads/2019/01/Security-Primer-EternalBlue.pdf

Upcoming Briefs

- *TrickBot and Ryuk*

- *Chinese State-sponsored Cyber Activity*

Product Evaluations

Recipients of this and other Healthcare Sector Cybersecurity Coordination Center (HC3) Threat Intelligence products are highly encouraged to provide feedback to **HC3@HHS.GOV**.

Requests for Information

Need information on a specific cybersecurity topic? Send your request for information (RFI) to **HC3@HHS.GOV** or call us Monday-Friday, between 9am-5pm (EST), at **(202) 691-2110.**

HC3 works with private and public sector partners to improve cybersecurity throughout the Healthcare and Public Health (HPH) Sector

Products

Sector & Victim Notifications

Directed communications to victims or potential victims of compromises, vulnerable equipment or PII/PHI theft and general notifications to the HPH about currently impacting threats via the HHS OIG

White Papers

Document that provides in-depth information on a cybersecurity topic to increase comprehensive situational awareness and provide risk recommendations to a wide audience.

Threat Briefings & Webinar

Briefing document and presentation that provides actionable information on health sector cybersecurity threats and mitigations. Analysts present current cybersecurity topics, engage in discussions with participants on current threats, and highlight best practices and mitigation tactics.

Need information on a specific cybersecurity topic or want to join our listserv? Send your request for information (RFI) to HC3@HHS.GOV or call us Monday-Friday, between 9am-5pm (EST), at **(202) 691-2110.**

Questions