Group 8 - Denis Yevstifeiv, Kobi Azarov and Adina Zuckerman

EternalBlue Vulnerability

What is EternalBlue?

EternalBlue is a cyberattack exploit developed by the US National Security Agency (NSA). It was leaked by the hacker group known as Shadow Brokers, on April 14th 2017, one month after Microsoft released patches for the vulnerability. The leak included many exploitation tools like EternalBlue, that are based on multiple vulnerabilities in the Windows implementation of SMB protocol.

EternalBlue works on all Windows versions prior to Windows 8. These versions contain an interprocess communication share (IPC) that allows a null session (a **null session** occurs when someone logs in to a system with no username or password). The NSA created a framework (much like Metasploit) named FuzzBunch, which was part of the leak.

Microsoft released patches for the vulnerabilities exposed in the leak, under the MS17-010 (Microsoft Security Bulletin).
https://docs.microsoft.com/en-us/security-updates/SecurityBulletins/2017/ms17-010

Technical descriptions

SMB Protocol
The Server Message Block (SMB) is a client server communication protocol that is a network file sharing protocol. This protocol allows applications on a computer to read and write to files, and request services from server programs in a computer network. The SMB protocol can be used on top of its TCP/IP protocol or other network protocols. The SMB protocol is intended for inter-network communication, which allows applications and services on networked computers to communicate.

Servers make file systems and other resources available to clients on the network. Client computers may have their own hard disk, but they also want access to the shared file systems and printers on the servers. Once they have established a connection, clients can then send commands to the server that allow them to access shares, open files, read and write files, and a variety of standard actions performed on a file system. However in the case of SMB these things are done over the network.

SMB1 vulnerability
The vulnerability exists because the SMB server, in various versions of Microsoft Windows, mishandles specially crafted packets from remote attackers, allowing them to execute arbitrary code on the target computer. The attackers used the vulnerability of that protocol to transfer files to each infected computer and execute code from the files.
The CVE (Common Vulnerabilities and Exposures) is CVE-2017-0144. This is insecure, when using SMB1 key protections offered by later SMB protocol versions are lost.

The NSA discovered the vulnerability in the Windows implementation of the **SMB protocol**. However, instead of reporting the vulnerability to Microsoft, it developed an exploit kit dubbed 'EternalBlue' to exploit the vulnerability.

It propagated through EternalBlue, an exploit developed by the NSA for older Windows systems. While Microsoft had released patches previously to close the exploit, much of WannaCry's spread was from organizations that had not applied these, or were using older Windows systems. WannaCry also took advantage of installing backdoors onto infected systems.

A Few of the CVEs related to the EternalBlue exploits:

Common Vulnerability Enumeration	Description
CVE-2017-0143	Windows SMB Remote Code Execution Vulnerability
CVE-2017-0144	Windows SMB Remote Code Execution Vulnerability
CVE-2017-0145	Windows SMB Remote Code Execution Vulnerability
CVE-2017-0146	Windows SMB Remote Code Execution Vulnerability
CVE-2017-0147	Windows SMB Information Disclosure Vulnerability
CVE-2017-0148	Windows SMB Remote Code Execution Vulnerability

How does the EternalBlue exploit work?

The exploit makes use of the way Microsoft Windows handles, or rather mishandles specially crafted packets from malicious attackers. All the attacker needs to do is

send a maliciously crafted packet to the target server, and voila, the malware propagtes and the cyberattack ensues.

Before Microsoft patching it, SMB version 1 was vulnerable to a buffer overflow attack. The vulnerability is exploitable when a malformed Trans2 request is sent to the server, which enables the attacker to overwrite another part of the memory. The goal of the attacker (and how NSA did it) would be to overwrite some useful memory portion and in this attack it is the buffer of another SMB connection, which enables arbitrary write and execution of shellcode in the memory address of the Hardware Abstraction Layer (HAL). In all Windows versions before Windows 10, the HAL is in a fixed memory address and is used during boot, therefore making it a nice target for the shellcode.

The exploit is happening in non-paged pool memory, which the SMB server allocates for the large requests sent to it. This is quite important information as we will soon see.

From the Metasploit and Worawits exploit, we can see that the primary exploit method works by creating multiple SMB connections, which makes the server reserve lots of space for the connections. This helps with aligning the data, so that the malicious packet is in a correct position to overflow to the next SMB connection. This process where filling up the heap, so that the malicious content would go to an advantageous position, is called **heap grooming**.

Example of the mishandeling

Memory Buffer Miscalculation: The vulnerability that EternalBlue exploits is quite subtle. One could easily miss it, if simply running a binary diffing tool against a patched and unpatched Srv.sys driver. Srv.sys is where large portions of the SMB protocol live, as Microsoft has opted to do many networking tasks in the kernel, perhaps for additional performance reasons. On most versions of Microsoft Windows, there is a function named srv!SrvOS2FeaListSizeToNt, which is used to calculate the size needed for a converting OS/2 Full Extended Attributes (FEA) List structures into the appropriate NT FEA structures. These structures are used to describe file characteristics. This calculation function is not present in Microsoft Windows 10, as it has been in-lined by the compiler. The vulnerability thus appears in srv!SrvOs2FeaListToNt.

Impact of vulnerability

At the end of 2018, millions of systems were still vulnerable to EternalBlue. This has led to millions of dollars in damages due primarily to ransomware worms. Following the massive impact of WannaCry, both NotPetya and BadRabbit caused over $1 billion worth of damages in over 65 countries, using EternalBlue as either an initial compromise vector or as a method of lateral movement.

> In May 2019, the city of Baltimore struggled with a cyberattack by digital extortionists; the attack froze thousands of computers, shut down email and disrupted real estate sales, water bills, health alerts and many other services. Nicole Perlroth, writing for the *New York Times*, initially attributed this attack to EternalBlue in a memoir published in February 2021, Perlroth clarified that EternalBlue had not been responsible for the Baltimore cyberattack, while criticizing others for pointing out "the technical detail that in this particular case, the ransomware attack had not spread with EternalBlue."
>
> Since 2012, four Baltimore City chief information officers have been fired or have resigned; two left while under investigation. Some security researchers said that the responsibility for the Baltimore breach lay with the city for not updating their computers. Security consultant Rob Graham wrote in a tweet: "If an organization has substantial numbers of Windows machines that have gone 2 years without patches, then that's squarely the fault of the organization, not EternalBlue.

Recommendation on how to fix/ mitigate EternalBlue

Anyone running versions of Windows Vista, Windows Server 2008, Windows 7, Windows Server 2008 R2, Windows 8. 1, Windows Server 2012 and Windows Server 2012 R2, Windows RT 8. 1, Windows 10, and Windows Server 2016 are all potentially vulnerable to the EternalBlue exploit.

The first thing that should be done to protect a system against the EternalBlue exploit is to install the MS17-010 patch issued by Microsoft in March 2017. MS17-010 is a security update that addresses the vulnerability by correcting how SMBv1 handles these specially crafted requests. Any systems running vulnerable Windows versions that did not install the patch should be immediately removed from all networks, until they are secured.

For any system using Windows XP, Windows Server 2003 or Windows 8, which are no longer supported by Microsoft, an emergency Windows patch, published by Microsoft, should be installed.

If it is not possible to install either one of the aforementioned patches, SMBv1 should be disabled, this is to prevent unauthorized access through this protocol.

If SMBv1 cannot be disabled, it should be blocked on network devices, UDP 137, 138 and TCP 139, 445.

If none of the above-mentioned options are available, the system should be shut down. This can help mitigate or prevent propagation.

In addition to installing the patch, it is crucial to make sure that the system is always up-to-date, by continuously updating and installing any recommended patches and software can help protect against attacks.

It is also important to perform regular backups for any system. It is best-practice to make sure the backup is stored off-site, or at least on an external system, not connected to the network. This ensures, in the event of an attack, that the information can be retrieved. It should be noted that backups are not always enough, since sensitive information in the hands of an attacker can be detrimental to an organization, even if the backups are intact.

Follow the least privilege principle. Access control should always be configured with the least privilege principle in mind. Users should remain in the privilege level required to suit their requirements, while allowing normal, suitable functioning. Limiting privileges won't necessarily protect against this type of vulnerability, however it can prevent malware from carrying out malicious tasks that require special privileges, such as deleting shadow copies of the infected system.

Controlling which executables have access to which files can also help mitigate the effects of an attack. Creating a whitelist of accessible files can prevent unauthorized programs from controlling other applications and systems, if they are not listed as "trusted". It's also important to establish policies based on trusts that will protect the whitelisted applications themselves from being corrupted or configured by illegitimate actors.

Case Studies

WannaCry and how it took advantage of this vulnerability

WannaCry is a ransomware worm. The attack occurred in May 2017. It is considered a network worm, because it also includes a "transport" mechanism to automatically spread itself. The attack spread rapidly through more than 200,000 computers across 150 countries.

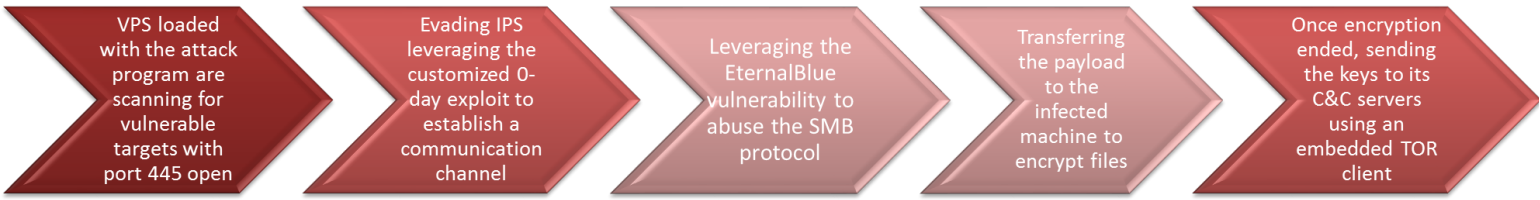
WannaCry's worm functionality comes from its use of the EternalBlue exploit, which takes advantage of a vulnerability in Windows' Server Message Block (SMB) protocol. After EternalBlue was leaked, Microsoft released an updated version of SMB that corrected the issue, in April 2017. While this was a month before the main WannaCry outbreak, many organizations had not yet installed the patch, making them vulnerable to WannaCry.

After a Machine is infected with WannaCry, it proceeds to scan the network for other machines running a vulnerable version of SMB. If one is found, the infected computer uses EternalBlue to send and run a copy of WannaCry on the targeted computer. At this point, the malware could begin encryption of the computer's files.

WannaCry is designed to deny a user access to their files on a computer unless a ransom is paid. This is accomplished through the use of encryption, where the malware transforms the data in a way that is only reversible with knowledge of the secret key. Since WannaCry's secret key is only known to the ransomware operator, this forces a victim to pay the ransom to retrieve their data. WannaCry is designed to search for and encrypt a set list of file extension types on a computer. The WannaCry malware demanded a ransom of US$300 from its victims. However, the ransom demand was to be paid in Bitcoin.

If a victim of a WannaCry attack pays the ransom, they *should* be provided with a decryption key for their computer. This enables a decryption program provided by the cybercriminals to reverse the transformation performed on the user's files and return access to the original data.

The WannaCry ransomware attack had a substantial financial impact worldwide. It is estimated this cybercrime caused $4 billion in losses across the globe.



Additional Information
It is very simple for a hacker to use the vulnerability as an example of something he could do to gain access to an smb (just an example not connected to the EternalBlue).

After acquiring the wanted ip the hacker will begin by Nmaping the server.
Let's say the IP is 192.168.1.1 for convenience purposes they use the command
Nmap -vv -A -sS -p- 192.168.1.1
To scan all ports -p-
To stealth scan -sS considered a stealth scan because it orders the nmap not to complete the three way handshake.
To get more information about the process and the ports -vv.
Enables OS detection version detection script detection and traceroute all in one -A

After mapping the network and seeing that either port number 139 or 445 is open the hacker will try to enumerate using Enum4Linux, which is a tool used to enumerate SMB shares on both windows and linux systems.

The code would look like this:
Enum4linux -A 192.168.1.1
-A gets userlist machine list namelist dump sharelist password policy information get group and member list.

Once the hacker acquired the information they needed, such sharfiles, they will most likely use some sort of exploit, such as mentioned above or the cve-2017-7494, that allow remote code execution or exploiting misconfiguration in the SMB server.

At this point, after the username and share is known, the attacker can try to connect to this specific share using the SMB client syntax.
For example: smbclient //192.168.1.1/(sharename) -U (user) -p (port number), perhaps betting on 'anonymous' as the username for the connection. At that point, if the combination worked they will have the possibility to access files that in some cases may contain usernames, password, RSA keys and even files such as the SSH files.

After this point they will have the option to escalate their privileges by using the data they retrieved and propagate an attack, limited only by their imagination.

Sources

https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2017-0144
https://research.checkpoint.com/2017/eternalblue-everything-know/
https://www.avast.com/c-eternalblue?v=rb
https://www.cvedetails.com/cve/CVE-2017-0143/
https://nvd.nist.gov/vuln/detail/CVE-2017-0144
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-0144
https://en.wikipedia.org/wiki/EternalBlue
https://www.exploit-db.com/docs/48760
https://risksense.com/wp-content/uploads/2018/05/White-Paper_Eternal-Blue.pdf
https://www.bswllc.com/resources-articles-5-immediate-steps-to-take-to-mitigate-a-wannacry-attack
https://docs.microsoft.com/en-us/security-updates/securitybulletins/2017/ms17-010
https://medium.com/@lucideus/the-eternal-exploitation-bible-lucideus-research-20e3ed541d4