Unraveling EternalBlue: inside the WannaCry's enabler

By Cybernews Team

Published: 2023-09-01 · Archived: 2026-04-15 02:09:37 UTC

WannaCry and NotPetya, probably two most damaging cyberattacks in recent history, were both only made possible because of EternalBlue. Here is how the NSA-developed cyber monster works, and how you should defend against it.

What is the EternalBlue vulnerability?

EternalBlue is a Windows exploit created by the US National Security Agency (NSA) and used in the 2017 WannaCry ransomware attack.

EternalBlue exploits a vulnerability in the Microsoft implementation of the Server Message Block (SMB) Protocol. This dupes a Windows machine that has not been patched against the vulnerability into allowing illegitimate data packets into the legitimate network. These data packets can contain malware such as a trojan, ransomware, or similar dangerous program.

The SMB Protocol is a standard, system that creates a connection between client and server by sending responses and requests. When printing a document, a person may use their computer, the client, to send a request to a colleague's computer, the server, with a request to print the document. The client and server communicate over the SMB Protocol.

The NSA did not alert Microsoft about EternalBlue's existence for a period of five years, until a breach of the NSA compelled the agency to do so. Microsoft blames the agency for EternalBlue's existence and its fallout, even though EternalBlue is based on what was then a Windows vulnerability. The NSA has declined to speak in detail about the hack or EternalBlue.

By Avast/Cybernews

How would EternalBlue look in a real attack scenario?

Imagine a large organization with a network infrastructure comprising multiple interconnected systems, including servers, workstations, and IoT devices. Within this network, there is a vulnerable Windows system that has not been patched with the necessary security updates to protect against EternalBlue.

A bad actor, seeking to exploit the vulnerability, initiates an attack by sending a specially crafted network packet to the vulnerable system. This packet contains the exploit code that takes advantage of the EternalBlue vulnerability, allowing the attacker to gain unauthorized access and execute arbitrary code on the compromised system.

Recon process

In the first stage of a cyberattack, a bad actor may employ various methods to identify systems vulnerable to the EternalBlue vulnerability. Here are a few techniques they might use:

- **Scanning for Open Ports:** The bad actor could use port scanning tools like Nmap to identify systems with open ports, such as SMB (Server Message Block) ports (e.g., port 445). By scanning a range of IP addresses, they can identify potential targets that have SMB services exposed to the internet.

The image below shows successful finding of EternalBlue vulnerability using **nmap**


Discovering EternalBlue

Cybernews screenshot

- **Exploit Frameworks:** There are well-known exploit frameworks like Metasploit that contain modules specifically designed to exploit the EternalBlue vulnerability. These frameworks provide a wide range of tools and exploits for attackers to leverage, including EternalBlue. By using such frameworks, the attacker can automate the process of identifying vulnerable systems and launching attacks.

The image below shows prebuilt EternalBlue exploits


EternalBlue exploits

Cybernews screenshot

- **Shodan and Similar Tools:** Shodan is a search engine that scans and indexes internet-connected devices, including vulnerable systems. By using specific search queries, an attacker can identify systems that are potentially susceptible to EternalBlue. Similar tools or databases listing vulnerable systems can also aid in identifying targets.
- **Targeted Phishing and Social Engineering:** In some cases, attackers may employ targeted phishing emails or social engineering techniques to gain initial access to a system within the target network. Once they've compromised a user's device, they can then perform internal network reconnaissance to find vulnerable systems and exploit EternalBlue.

It's important to note that discovering vulnerable systems is only the first step for bad actors. Once they identify a vulnerable system, they proceed to exploit the vulnerability, gain access, and then move laterally within the network to escalate privileges and achieve their objectives

Exploit execution

Once the target system is identified, the attacker launches an exploit against the vulnerable system. One of the most popular exploitation tools is Metasploit Framework.

What is Metasploit Framework?

The Metasploit Framework is a Ruby-based, modular penetration testing platform that enables you to write, test, and execute exploit code. The Metasploit Framework contains a suite of tools that you can use to test security vulnerabilities, enumerate networks, execute attacks, and evade detection. At its core, the Metasploit Framework is a collection of commonly used tools that provide a complete environment for penetration testing and exploit development.

Metasploit Framework has anEternalBlue exploit, which can be used directly to exploit vulnerable system

 EternalBlue exploit

Cybernews screenshot

The image below shows successful exploitation of the EternalBlue vulnerability

 Successful EternalBlue exploitation

Cybernews screenshot

EternalBlue takes advantage of three different bugs. The first is a mathematical error when the protocol tries to cast an OS/2 FileExtended Attribute (FEA) list structure to an NT FEA structure in order to determine how much memory to allocate. A miscalculation creates an integer overflow that causes less memory to be allocated than expected, which in turns leads to a buffer overflow.

With more data than expected being written, the extra data can overflow into adjacent memory space triggering the buffer overflow. This is achieved thanks to the second bug, which results from a difference in the SMB protocol's definition of two related sub commands: SMB_COM_TRANSACTION2 and SMB_COM_NT_TRANSACT.

Both have a _SECONDARY command that is used when there is too much data to include in a single packet. The crucial difference between TRANSACTION2 and NT_TRANSACT is that the latter calls for a data packet twice the size of the former. This is significant because an error in validation occurs if the client sends a crafted message using the NT_TRANSACT sub-command immediately before the TRANSACTION2 one.

While the protocol recognizes that two separate sub-commands have been received, it assigns the type and size of both packets (and allocates memory accordingly) based only on the type of the last one received. Since the last one is smaller, the first packet will occupy more space than it is allocated.

Once the attackers achieve this initial overflow, they can take advantage of a third bug in SMBv1 which allows heap spraying, a technique which results in the allocation of a chunk of memory at a given address. From here, the attacker can write and execute shellcode to take control of the system.

Upon successfully compromising the initial system, the attacker begins their reconnaissance phase. They explore the network, scanning for other vulnerable systems or potential targets. Using tools like Nmap or Metasploit, the attacker identifies additional systems with unpatched vulnerabilities, possibly even finding weak or default credentials that grant further access.

 EternalBlue privilege escalation

Cybernews screenshot


EternalBlue privilege escalation 2

Cybernews screenshot

The image below shows successful privilege escalation


EternalBlue privilege escalation 3

The lateral movement phase

With a growing foothold within the organization's network, the attacker starts to escalate privileges and move laterally, traversing from one compromised system to another. They may use techniques like Pass-the-Hash or Pass-the-Ticket to escalate privileges and impersonate legitimate users, enabling them to access more sensitive resources and expand their control over the network.

During this lateral movement, the attacker may deploy various tools and malware to further their objectives. For example, they might use keyloggers or credential-stealing malware to harvest login credentials of high-privileged users, allowing them to gain even greater control over critical systems and sensitive data.

In some instances, the attacker might choose to deploy ransomware across the network, encrypting important files and bringing operations to a halt. They then demand a ransom in exchange for the decryption keys, causing financial losses and potential reputational damage to the organization.

Throughout this entire process, the attacker may operate stealthily, attempting to evade detection by leveraging anti-forensic techniques and obfuscating their activities. They might use encryption and tunneling techniques to hide their network traffic and maintain persistence within the compromised systems to ensure long-term access.

Does EternalBlue still exist?

Yes, there are 4332 servers or Operating systems exposed on the internet with EternalBlue vulnerability.

The Top 10 countries that have systems with EternalBlue vulnerability:


Top 10 countries with EternalBlue vulnerability

Top Operating systems vulnerable to EternalBlue:

- Windows 7 Professional 7600
- Windows 8.1 Pro 9600
- Windows Server 2021 R2 Standard


Operating systems vulnerable to EternalBlue

How to defend against EternalBlue?

To protect against the EternalBlue vulnerability, it’s crucial to implement the following measures:

- **Patching and Updates:** Apply security patches and updates promptly. Microsoft released patches for the EternalBlue vulnerability in March 2017. Ensure that all affected systems, including servers and workstations, have the necessary updates installed. Additionally, keep all software, operating systems, and network devices up to date with the latest security patches.
- **Disable SMBv1:** Since EternalBlue targets the SMBv1 protocol, consider disabling or blocking SMBv1 across your network, especially if it is not required. SMBv2 or SMBv3 should be used as more secure alternatives.
- **Network Segmentation:** Implement network segmentation to isolate critical systems and restrict access between different parts of the network. This reduces the lateral movement potential of attackers and contains the impact of any successful exploitation.
- **Firewalls and Intrusion Detection Systems:** Configure firewalls to block suspicious network traffic and restrict unnecessary access to SMB services. Intrusion Detection Systems (IDS) and Intrusion Prevention Systems (IPS) can help detect and block exploit attempts targeting the EternalBlue vulnerability.
- **Access Controls and Privilege Management:** Enforce strong access controls and least privilege principles. Limit user privileges to only what is necessary for their roles, and regularly review and revoke unnecessary privileges. This reduces the potential impact of an attacker who successfully exploits the vulnerability.
- **Security Awareness and User Education:** Train users to recognize and report phishing emails and suspicious attachments. Promote security awareness and educate users about the risks of clicking on unknown links or opening attachments from untrusted sources, as these can be entry points for attacks.
- **Endpoint Protection:** Deploy and maintain reliable antivirus and anti-malware solutions on all systems. Ensure that these security tools are regularly updated with the latest threat definitions to detect and block known malware that may utilize EternalBlue or similar vulnerabilities.
- **Network Monitoring and Incident Response:** Implement robust network monitoring and logging capabilities to detect and respond to any potential exploitation attempts or suspicious activity. Have an incident response plan in place to quickly respond and mitigate the impact if an exploitation occurs.

Summary

EternalBlue has been widely exploited by bad actors for various malicious activities, including ransomware attacks, botnet creation, credential theft, and lateral movement within networks. Its exploitation can have serious consequences, resulting in data breaches, financial losses, operational disruption, and reputation damage to organizations.

The flaw affects a wide range of Windows operating systems, including older versions like Windows XP and Windows Server 2003, which were still in use by many organizations at the time of its discovery. The widespread presence increased the potential attack surface and made it a critical concern for security professionals.

EternalBlue gained notable attention through its involvement in prominent cyber attacks. The WannaCry ransomware outbreak in 2017 infected hundreds of thousands of systems worldwide, causing widespread disruption in various sectors such as healthcare, government, and financial services. The NotPetya malware, another highly impactful cyber attack, also leveraged EternalBlue for propagation.

EternalBlue has a worm-like capability, allowing it to propagate within networks without user interaction. This self-spreading feature facilitated the rapid propagation of malware, enabling attackers to compromise vulnerable systems quickly and effectively.