Graham Dungan
April 20, 2025
UIN: 332001764

CSCE 413: Software Security
Self-Study: EternalBlue

What is the Vulnerability?
EternalBlue is a Kernel-level exploit of a vulnerability within the Server Message Block (SMB) file sharing protocol by Microsoft. EternalBlue was released/disclosed in March 2017 by a group known as the Shadow Brokers, who claimed that they stole it from the NSA. SMB itself allows the manipulation (read, write, etc.) of files over a network. EternalBlue uses a vulnerability within this protocol to perform remote code execution on machines in the same network. This exploit is notorious for its transmissibility and has been used in multiple larger pieces of malware since its theft and release.

What was the Root Cause?
SMB, much like PingOfDeath, has a transaction mechanism named Trans (or Trans2) that allows for the fragmentation of a large data payload across multiple networks. The vulnerability itself lies within how the SMB server reassembles the fragmented messages. Whenever a message is received, the server implicitly trusts the `TotalDataCount`, `DataOffset`, and `DataCount` fields in the SMB headers instead of performing bounds checking on the actual data against the buffer. Since the server does not validate that the data can fit within the buffer, a malicious user can craft a malicious payload that falsifies its offset/size (when fragmented), performing a buffer overflow. Since the system needs to reassemble packets before they are authenticated, this attack allows for a near-instant RCE on machines without the need for authentication.

What is the Extent of its Impact?
EternalBlue is known throughout the world of cybersecurity due to its notable presence within many different forms of malware. This first major use of EternalBlue was in the world-wide WannaCry ransomware outbreak which affected thousands of machines rendering businesses inoperable. In the same year, EternalBlue was used in a malware called NotPetya in Ukraine, effectively shutting down most of the country's infrastructure and businesses. Later in 2017 EternalBlue was found in the EternalRocks malware/worm that contained other tools created by the NSA. EternalBlue had become so popular so quickly that it was integrated into many toolsets like Metasploit for exploitation of non-patched machines.
Beyond the impact of the vulnerability in a machine-sense, the political and social impacts EternalBlue had were just as notable. EternalBlue shed light on the NSA's failure to disclose critical vulnerabilities to Microsoft. Instead, the NSA had kept the vulnerability to be used against persons of interest. This entire ordeal caused the public to reconsider their trust in some aspects of the NSA's operations and for cybersecurity experts to redefine the importance of disclosures for protecting the public.

How to Patch it?
Like all buffer overflows, the patch for EternalBlue was rather underwhelming. The patch for this vulnerability came in `MS17-010`, which addressed EternalBlue, memory corruption, and DoublePulsar (another vulnerability used in WannaCry and NotPetya, developed by the NSA). This patch added strict bounds checking during fragment assembly and more defensive checks for other features.

How Could it Have Been Prevented?
EternalBlue could have been prevented in two ways. Firstly, a 0-trust policy must be in place for any received data. Even if data is acquired via some authenticated machine or user, it still should be scrutinized for errors and malicious intent. An accidental use of SMB with packets could have caused the same error; the only difference in EternalBlue's case was intent. The second way this could have been prevented was through disclosure from the NSA. A vulnerability is a vulnerability, and to purposefully keep the public vulnerable in the same way an attacker may be is a failure to protect. It is the responsibility of those who find such vulnerabilities to properly disclose them.

References

1. EternalBlue - Wikipedia
2. EternalBlue - Hypr
3. What Is EternalBlue and Why Is the MS17-010 Exploit Still Relevant? - Avast
4. SMB Exploited: WannaCry Use of "EternalBlue" - Google Cloud