EternalBlue

CVE-2017-0143

MS17-010

Group 8 -
Denis Yevstifeiv, Kobi Azarov and Adina Zuckerman

What is EternalBlue?

EternalBlue is a cyberattack exploit developed by the NSA. It was leaked by Shadow Brokers, on April 14th 2017, one month after Microsoft released patches for the vulnerability. EternalBlue is based on multiple vulnerabilities in the Windows implementation of SMB protocol.

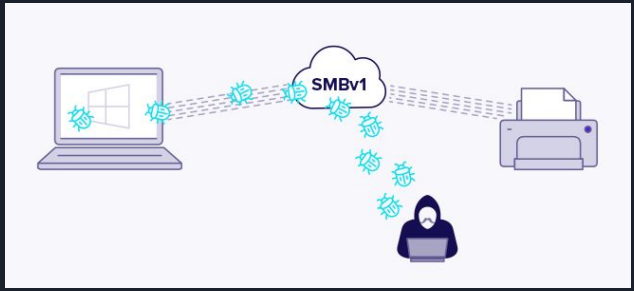
EternalBlue works on all Windows versions prior to Windows 8.

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).

How does the Eternalblue functions

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 propagates and the cyber attack ensues.



Recommendation on How to Fix/ Mitigate EternalBlue

The first step that should be taking is to install the MS17-010 patch issued by Microsoft in March 2017, protect a system against the EternalBlue exploit. Microsoft published emergency patches for systems which are no longer supported by the company.

If installing the patches is not possible, SMBv1 should be disabled, or blocked, and in extreme situations where this is not possible, shut down the system to mitigate the potential risk to the network.

Perform regular backups on the system to reduce the risks presented by ransomware attacks.

Configure access control and proper privileges.

Control the reach of executable files.

Case Study - WannaCry

WannaCry is a ransomware worm. The attack occurred in May 2017 and 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 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.

Case Study - WannaCry

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 encrypts the data in a way that is only reversible with knowledge of the secret key. The attackers demanded payment from the victims in order to retrieve their data. 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.

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