EternalBlue

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, generally secure 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 are communicating 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.

EternalBlue was among the information spilled by a hacking group called the **Shadow Brokers**, who in 2017 hacked an NSA trove of cyber weapons. Shadow Brokers published EternalBlue on the internet causing chaos and embarrassment for the NSA. Microsoft was advised and took action by urgently sharing a security **patch** for Windows sysadmins. Those whose systems were unpatched or who were running older Windows versions were left open to attacks.

At the time the dominant Windows versions were 7 and 10, although some large enterprises were still using Windows XP. During the WannaCry event that occurred just weeks after the leak of NSA breach content, Microsoft (upon NSA notice) had already released a patch for Windows versions 7 and 10. The company then released a patch for the otherwise-unsupported Windows XP.

Example:

“I was a sysadmin during the WannaCry incident where hackers used EternalBlue to deploy ransomware against enterprises with Windows environments. It was a rough time but my then-employer and I ran a tight ship. We implemented the Windows 10 patch immediately and were protected.”

EternalBlue Explained:

EternalBlue Exploit Against Windows 7 (MS17-010)

← Escrow Passwords

Extensible Authentication Protocol (EAP) →

Search for a Topic

A B C D E F G H I K L M N O P Q R S T U V W Z

Popular Pages

Identity Verification

Identity Assurance

Rainbow Table Attack

Keylogger

Share This Post

Identity Security Starts Here
• Eliminate authentication attacks
• Actively combat identity risks
• Reduce identity fraud
GET A DEMO

Platform

Identity Assurance Platform

HYPR Authenticate

HYPR Adapt

HYPR Affirm

HYPR Enterprise Passkeys

Integrations

Pricing

Solutions

For Your Workforce

For Your Customers

Cyber Insurance MFA

Deploy Passkeys

PSD2 SCA

Zero Trust Authentication

Critical Infrastructure

Financial Services

Accessibility

Vulnerability Disclosure

Resources

Resource Center

Blog

Passwordless Guide

Security Encyclopedia

Company

See Why Identity Security Starts Here

GET A DEMO

Receive Updates and News from HYPR

Enter Your Email

SUBMIT