EternalBlue

From Wikipedia, the free encyclopedia

[Jump to navigation](https://en.wikipedia.org/wiki/EternalBlue#mw-head)[Jump to search](https://en.wikipedia.org/wiki/EternalBlue#searchInput)

|  |  |
| --- | --- |
|  | This article **provides insufficient context for those unfamiliar with the subject**. Please help [improve the article](https://en.wikipedia.org/w/index.php?title=EternalBlue&action=edit) by [providing more context for the reader](https://en.wikipedia.org/wiki/Wikipedia:Writing_better_articles#Provide_context_for_the_reader). *(July 2018) (*[*Learn how and when to remove this template message*](https://en.wikipedia.org/wiki/Help:Maintenance_template_removal)*)* |

|  |  |
| --- | --- |
| **Eternal Exploit** | |
| **Common name** | Eternal |
| **Technical name** | * **Blue Variant**   + Trojan:Win32/EternalBlue ([Microsoft](https://en.wikipedia.org/wiki/Microsoft)) [[1]](https://en.wikipedia.org/wiki/EternalBlue#cite_note-1) * **Rocks Variant**   + TrojanDownloader:Win32/Eterock.[Letter] ([Microsoft](https://en.wikipedia.org/wiki/Microsoft)) [[2]](https://en.wikipedia.org/wiki/EternalBlue#cite_note-2)   + W32.Eternalrocks ([Symantec](https://en.wikipedia.org/wiki/NortonLifeLock)) [[3]](https://en.wikipedia.org/wiki/EternalBlue#cite_note-3)   + TROJ\_ETEROCK.[Letter] ([Trend Micro](https://en.wikipedia.org/wiki/Trend_Micro)) [[4]](https://en.wikipedia.org/wiki/EternalBlue#cite_note-4)   + Mal/Eterocks-[Letter] ([Sophos](https://en.wikipedia.org/wiki/Sophos))   + Troj/Eterocks-[Letter] (Sophos) * **Synergy Variant**   + Win32/Exploit.Equation.EternalSynergy ([ESET](https://en.wikipedia.org/wiki/ESET)) [[5]](https://en.wikipedia.org/wiki/EternalBlue#cite_note-5) |
| **Type** | [Vulnerability](https://en.wikipedia.org/wiki/Vulnerability) |
| **Author(s)** | [Equation Group](https://en.wikipedia.org/wiki/Equation_Group) |
| [**Operating system(s)**](https://en.wikipedia.org/wiki/Operating_system)**affected** | [Windows 95](https://en.wikipedia.org/wiki/Windows_95), [Windows 98](https://en.wikipedia.org/wiki/Windows_98), [Windows Me](https://en.wikipedia.org/wiki/Windows_Me), [Windows NT](https://en.wikipedia.org/wiki/Windows_NT), [Windows 2000](https://en.wikipedia.org/wiki/Windows_2000), [Windows XP](https://en.wikipedia.org/wiki/Windows_XP) |

**EternalBlue**[[6]](https://en.wikipedia.org/wiki/EternalBlue#cite_note-ars-6) is a [cyberattack](https://en.wikipedia.org/wiki/Cyberweapon) [exploit](https://en.wikipedia.org/wiki/Exploit_(computer_security)) developed by the U.S. [National Security Agency](https://en.wikipedia.org/wiki/National_Security_Agency) (NSA).[[7]](https://en.wikipedia.org/wiki/EternalBlue#cite_note-7) It was leaked by the [Shadow Brokers](https://en.wikipedia.org/wiki/The_Shadow_Brokers) hacker group on April 14, 2017, one month after Microsoft released patches for the [vulnerability](https://en.wikipedia.org/wiki/Vulnerability_(computing)).

On May 12, 2017, the worldwide [WannaCry ransomware](https://en.wikipedia.org/wiki/WannaCry_ransomware) used this exploit to attack unpatched computers.[[6]](https://en.wikipedia.org/wiki/EternalBlue#cite_note-ars-6)[[8]](https://en.wikipedia.org/wiki/EternalBlue#cite_note-8)[[9]](https://en.wikipedia.org/wiki/EternalBlue#cite_note-9)[[10]](https://en.wikipedia.org/wiki/EternalBlue#cite_note-:0-10)[[11]](https://en.wikipedia.org/wiki/EternalBlue#cite_note-11)[[12]](https://en.wikipedia.org/wiki/EternalBlue#cite_note-Wired_5-7-12):1 On June 27, 2017, the exploit was again used to help carry out the [2017 NotPetya cyberattack](https://en.wikipedia.org/wiki/2017_NotPetya_cyberattack) on more unpatched computers.[[13]](https://en.wikipedia.org/wiki/EternalBlue#cite_note-13)

The exploit was also reported to have been used since March 2016 by the Chinese hacking group [Buckeye (APT3)](https://en.wikipedia.org/wiki/Advanced_persistent_threat#APT_groups), after they likely found and re-purposed the tool,[[12]](https://en.wikipedia.org/wiki/EternalBlue#cite_note-Wired_5-7-12):1 as well as reported to have been used as part of the Retefe banking [trojan](https://en.wikipedia.org/wiki/Trojan_horse_(computing)) since at least September 5, 2017.[[14]](https://en.wikipedia.org/wiki/EternalBlue#cite_note-14)

EternalBlue was among the several exploits used, in conjunction with the [DoublePulsar](https://en.wikipedia.org/wiki/DoublePulsar) [backdoor](https://en.wikipedia.org/wiki/Backdoor_(computing)) implant tool.[[15]](https://en.wikipedia.org/wiki/EternalBlue#cite_note-15)



**Contents**

* [1Details](https://en.wikipedia.org/wiki/EternalBlue#Details)
* [2Responsibility](https://en.wikipedia.org/wiki/EternalBlue#Responsibility)
* [3EternalRocks](https://en.wikipedia.org/wiki/EternalBlue#EternalRocks)
  + [3.1Infection](https://en.wikipedia.org/wiki/EternalBlue#Infection)
* [4See also](https://en.wikipedia.org/wiki/EternalBlue#See_also)
* [5References](https://en.wikipedia.org/wiki/EternalBlue#References)
* [6Further reading](https://en.wikipedia.org/wiki/EternalBlue#Further_reading)
* [7External links](https://en.wikipedia.org/wiki/EternalBlue#External_links)

Details[[edit](https://en.wikipedia.org/w/index.php?title=EternalBlue&action=edit&section=1)]

EternalBlue exploits a vulnerability in [Microsoft](https://en.wikipedia.org/wiki/Microsoft)'s implementation of the [Server Message Block](https://en.wikipedia.org/wiki/Server_Message_Block) (SMB) protocol. This vulnerability is denoted by entry [CVE](https://en.wikipedia.org/wiki/CVE_(identifier))-[2017-0144](https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-0144)[[16]](https://en.wikipedia.org/wiki/EternalBlue#cite_note-16)[[17]](https://en.wikipedia.org/wiki/EternalBlue#cite_note-17) in the [Common Vulnerabilities and Exposures](https://en.wikipedia.org/wiki/Common_Vulnerabilities_and_Exposures) (CVE) catalog. The vulnerability exists because the SMB version 1 (SMBv1) server in various versions of [Microsoft Windows](https://en.wikipedia.org/wiki/Microsoft_Windows) mishandles specially crafted packets from remote attackers, allowing them to execute arbitrary code on the target computer.[[18]](https://en.wikipedia.org/wiki/EternalBlue#cite_note-18)

The NSA did not alert Microsoft about the vulnerabilities, and held on to it for more than five years before the breach forced its hand. The agency then warned Microsoft after learning about EternalBlue’s possible theft, allowing the company to prepare a software patch issued in March 2017,[[19]](https://en.wikipedia.org/wiki/EternalBlue#cite_note-19) after delaying its regular release of security [patches](https://en.wikipedia.org/wiki/Patch_Tuesday) in February 2017.[[20]](https://en.wikipedia.org/wiki/EternalBlue#cite_note-verge-nsapatch-20) On [Tuesday](https://en.wikipedia.org/wiki/Patch_Tuesday), March 14, 2017, Microsoft issued security bulletin MS17-010,[[21]](https://en.wikipedia.org/wiki/EternalBlue#cite_note-microsoft.com-21) which detailed the flaw and announced that [patches](https://en.wikipedia.org/wiki/Security_patch) had been released for all Windows versions that were currently supported at that time, these being [Windows Vista](https://en.wikipedia.org/wiki/Windows_Vista), [Windows 7](https://en.wikipedia.org/wiki/Windows_7), [Windows 8.1](https://en.wikipedia.org/wiki/Windows_8.1), [Windows 10](https://en.wikipedia.org/wiki/Windows_10), [Windows Server 2008](https://en.wikipedia.org/wiki/Windows_Server_2008), [Windows Server 2012](https://en.wikipedia.org/wiki/Windows_Server_2012), and [Windows Server 2016](https://en.wikipedia.org/wiki/Windows_Server_2016).[[22]](https://en.wikipedia.org/wiki/EternalBlue#cite_note-22)[[23]](https://en.wikipedia.org/wiki/EternalBlue#cite_note-23) The next day, Microsoft released emergency security patches for the unsupported [Windows XP](https://en.wikipedia.org/wiki/Windows_XP), [Windows 8](https://en.wikipedia.org/wiki/Windows_8), and [Windows Server 2003](https://en.wikipedia.org/wiki/Windows_Server_2003).[[24]](https://en.wikipedia.org/wiki/EternalBlue#cite_note-24)[[25]](https://en.wikipedia.org/wiki/EternalBlue#cite_note-25)

Many Windows users had not installed the patches when, two months later on May 12, 2017, the [WannaCry ransomware attack](https://en.wikipedia.org/wiki/WannaCry_ransomware_attack) used the EternalBlue vulnerability to spread itself.[[26]](https://en.wikipedia.org/wiki/EternalBlue#cite_note-26)[[27]](https://en.wikipedia.org/wiki/EternalBlue#cite_note-27)

In February 2018, EternalBlue was ported to all Windows operating systems since [Windows 2000](https://en.wikipedia.org/wiki/Windows_2000) by [RiskSense](https://en.wikipedia.org/w/index.php?title=RiskSense&action=edit&redlink=1) security researcher Sean Dillon. [EternalChampion](https://en.wikipedia.org/w/index.php?title=EternalChampion&action=edit&redlink=1) and [EternalRomance](https://en.wikipedia.org/w/index.php?title=EternalRomance&action=edit&redlink=1), two other exploits originally developed by the NSA and leaked by [The Shadow Brokers](https://en.wikipedia.org/wiki/The_Shadow_Brokers), were also ported at the same event. They were made available as [open sourced](https://en.wikipedia.org/wiki/Open-source_model) [Metasploit](https://en.wikipedia.org/wiki/Metasploit) modules.[[28]](https://en.wikipedia.org/wiki/EternalBlue#cite_note-28)

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](https://en.wikipedia.org/wiki/WannaCry), both [NotPetya](https://en.wikipedia.org/wiki/NotPetya) and [BadRabbit](https://en.wikipedia.org/w/index.php?title=BadRabbit&action=edit&redlink=1) 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.[[29]](https://en.wikipedia.org/wiki/EternalBlue#cite_note-29)

In May 2019, the city of [Baltimore](https://en.wikipedia.org/wiki/Baltimore) struggled with a cyberattack by digital extortionists using EternalBlue. The attack froze thousands of computers, shut down email and disrupted real estate sales, water bills, health alerts and many other services.[[30]](https://en.wikipedia.org/wiki/EternalBlue#cite_note-30) Since 2012, four Baltimore City chief information officers have been fired or have resigned; two left while under investigation.[[31]](https://en.wikipedia.org/wiki/EternalBlue#cite_note-31) 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."[[32]](https://en.wikipedia.org/wiki/EternalBlue#cite_note-32)

Responsibility[[edit](https://en.wikipedia.org/w/index.php?title=EternalBlue&action=edit&section=2)]

According to [Microsoft](https://en.wikipedia.org/wiki/Microsoft), it was the United States's [NSA](https://en.wikipedia.org/wiki/National_Security_Agency) that was responsible because of its controversial strategy of not disclosing but stockpiling vulnerabilities. The strategy prevented Microsoft from knowing of (and subsequently patching) this bug, and presumably other hidden bugs.[[33]](https://en.wikipedia.org/wiki/EternalBlue#cite_note-33)[[34]](https://en.wikipedia.org/wiki/EternalBlue#cite_note-34)

EternalRocks[[edit](https://en.wikipedia.org/w/index.php?title=EternalBlue&action=edit&section=3)]

**EternalRocks** or **MicroBotMassiveNet** is a [computer worm](https://en.wikipedia.org/wiki/Computer_worm) that infects Microsoft Windows. It uses seven exploits developed by the NSA.[[35]](https://en.wikipedia.org/wiki/EternalBlue#cite_note-cnet-35) Comparatively, the WannaCry [ransomware](https://en.wikipedia.org/wiki/Ransomware) program that infected 230,000 computers in May 2017 only uses two NSA exploits, making researchers believe EternalRocks to be significantly more dangerous.[[36]](https://en.wikipedia.org/wiki/EternalBlue#cite_note-36) The worm was discovered via [honeypot](https://en.wikipedia.org/wiki/Honeypot_(computing)).[[37]](https://en.wikipedia.org/wiki/EternalBlue#cite_note-37)

**Infection**[[edit](https://en.wikipedia.org/w/index.php?title=EternalBlue&action=edit&section=4)]

EternalRocks first installs [Tor](https://en.wikipedia.org/wiki/Tor_(anonymity_network)), a private network that conceals Internet activity, to access its hidden servers. After a brief 24 hour "[incubation period](https://en.wikipedia.org/wiki/Incubation_period)",[[35]](https://en.wikipedia.org/wiki/EternalBlue#cite_note-cnet-35) the server then responds to the malware request by downloading and self-replicating on the "[host](https://en.wikipedia.org/wiki/Host_(biology))" machine.

The malware even names itself WannaCry to avoid detection from security researchers. Unlike WannaCry, EternalRocks does not possess a [kill switch](https://en.wikipedia.org/wiki/Kill_switch) and is not ransomware.[[35]](https://en.wikipedia.org/wiki/EternalBlue#cite_note-cnet-35)

See also[[edit](https://en.wikipedia.org/w/index.php?title=EternalBlue&action=edit&section=5)]

* [BlueKeep (security vulnerability)](https://en.wikipedia.org/wiki/BlueKeep_(security_vulnerability)) – A similar vulnerability
* [Petya (malware)](https://en.wikipedia.org/wiki/Petya_(malware))