MS-ISAC®
Multi-State Information Sharing & Analysis Center®

Security Primer
January 2019 • SP2019-0101

EternalBlue

EternalBlue is an exploit that allows cyber threat actors to remotely execute arbitrary code and gain access to a network by sending specially crafted packets. It exploits a software vulnerability in Microsoft's Windows operating systems (OS) Server Message Block (SMB) version 1 (SMBv1) protocol, a network file sharing protocol that allows access to files on a remote server. This exploit potentially allows cyber threat actors to compromise the entire network and all devices connected to it. Due to EternalBlue's ability to compromise networks, if one device is infected by malware via EternalBlue, every device connected to the network is at risk. This makes recovery difficult, as all devices on a network may have to be taken offline for remediation. This vulnerability was patched and is listed on Microsoft's security bulletin as MS17-010.

Malware that utilizes EternalBlue can self-propagate across networks, drastically increasing its impact. For example, WannaCry, a crypto-ransomware, was one of the first and most well-known malware to use this exploit to spread. WannaCry uses the EternalBlue exploit to spread itself across the network infecting all devices connected and dropping the cryptro-ransomware payload. This increased the persistence and damage that WannaCry could cause in a short amount of time. This increase has made EternalBlue popular with various malware, such as Trickbot, a modular banking trojan, as well as CoinMiner and WannaMine, cryptominers that use the EternalBlue exploit in order to gain access to computing power to mine cryptocurrencies.

For more information on this vulnerability, please see the MS-ISAC's Microsoft SMBv1 Advisory and the Common Vulnerabilities and Exposures list where it is listed under CVE-2017-0143, CVE-2017-0144, CVE-2017-0145, CVE-2017-0146, CVE-2017-0147, and CVE-2017-0148.

Recommendations

- Patch devices with Microsoft Windows OS with the security update for Microsoft Windows SMB v1. The Microsoft Security Bulletin, MS17-010, includes the list of affected Windows OS.
- Use Eset's tool to check whether your version of Windows is vulnerable.
- Where appropriate, disable SMBv1 on all systems and utilize SMBv2 or SMBv3, after appropriate testing.
- Use Group Policy Objects to set a Windows Firewall rule to restrict inbound SMB communication to client systems. If using an alternative host-based intrusion prevention system (HIPS), consider implementing custom modifications for the control of client-to-client SMB communication. At minimum create a Group Policy Object that restricts inbound SMB connections to clients originating from clients.
- Apply the Principle of Least Privilege to all systems and services and run all software as a non-privileged user (one without administrative privileges).

The *MS-ISAC* is the focal point for cyber threat prevention, protection, response, and recovery for the nation's state, local, tribal, and territorial (SLTT) governments. More information about this topic, as well as 24x7 cybersecurity assistance is available at 866-787-4722, *SOC@cisecurity.org*. The MS-ISAC is interested in your comments - an anonymous feedback *survey* is available.