CVE Report: CVE-2017-0144

# CVSS Score

CVSS Score: 8.8 HIGH

CVSS Vector: AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H

# Description

The SMBv1 server in Microsoft Windows Vista SP2; Windows Server 2008 SP2 and R2 SP1; Windows 7 SP1; Windows 8.1; Windows Server 2012 Gold and R2; Windows RT 8.1; and Windows 10 Gold, 1511, and 1607; and Windows Server 2016 allows remote attackers to execute arbitrary code via crafted packets, aka "Windows SMB Remote Code Execution Vulnerability." This vulnerability is different from those described in CVE-2017-0143, CVE-2017-0145, CVE-2017-0146, and CVE-2017-0148.

# Affected Assets

Vendor: Microsoft Corporation, Product: Windows SMB

# Exploits

Title: DOUBLEPULSAR - Payload Execution and Neutralization (Metasploit), Link: https://www.exploit-db.com/exploits/47456, Download: https://www.exploit-db.com/download/47456

Title: Microsoft Windows 7/8.1/2008 R2/2012 R2/2016 R2 - 'EternalBlue' SMB Remote Code Execution (MS17-010), Link: https://www.exploit-db.com/exploits/42315, Download: https://www.exploit-db.com/download/42315

Title: Microsoft Windows 8/8.1/2012 R2 (x64) - 'EternalBlue' SMB Remote Code Execution (MS17-010), Link: https://www.exploit-db.com/exploits/42030, Download: https://www.exploit-db.com/download/42030

Title: Microsoft Windows 7/2008 R2 - 'EternalBlue' SMB Remote Code Execution (MS17-010), Link: https://www.exploit-db.com/exploits/42031, Download: https://www.exploit-db.com/download/42031

Title: Microsoft Windows Server 2008 R2 (x64) - 'SrvOs2FeaToNt' SMB Remote Code Execution (MS17-010), Link: https://www.exploit-db.com/exploits/41987, Download: https://www.exploit-db.com/download/41987

Title: Microsoft Windows - SMB Remote Code Execution Scanner (MS17-010) (Metasploit), Link: https://www.exploit-db.com/exploits/41891, Download: https://www.exploit-db.com/download/41891