CVE Report for CVE-2017-0144

CVE Information

CVE ID: CVE-2017-0144

Summary: 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.

Base Score: 8.1 HIGH

Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H

Reference:

http://packetstormsecurity.com/files/154690/DOUBLEPULSAR-Payload-Execution-Neutralization.html

Affected Systems Information

Microsoft » Server Message Block » Version: 1.0
cpe:2.3:a:microsoft:server_message_block:1.0:*:*:*:*:*:*:*
Matching versions
When used together with: Microsoft » Windows 10
When used together with: Microsoft » Windows 10 » Version: 1511
When used together with: Microsoft » Windows 10 » Version: 1607
When used together with: Microsoft » Windows 7 » Version: N/A Update SP1
When used together with: Microsoft » Windows 8.1
When used together with: Microsoft » Windows Rt 8.1 » Version: N/A
When used together with: Microsoft » Windows Server 2008 » Version: N/A Update SP2
When used together with: Microsoft » Windows Server 2008 » Version: R2 Update SP1
When used together with: Microsoft » Windows Server 2012 » Version: N/A Update Gold
When used together with: Microsoft » Windows Server 2012 » Version: R2
When used together with: Microsoft » Windows Server 2016 » Version: N/A
When used together with: Microsoft » Windows Vista » Version: N/A Update SP2

Exploit Information

Exploit Links to Download:

https://www.exploit-db.com/download/47456
https://www.exploit-db.com/download/42315
https://www.exploit-db.com/download/42030

https://www.exploit-db.com/download/42031
https://www.exploit-db.com/download/41987
https://www.exploit-db.com/download/41891

Exploit Links to Look:

https://www.exploit-db.com/exploits/47456
https://www.exploit-db.com/exploits/42315
https://www.exploit-db.com/exploits/42030
https://www.exploit-db.com/exploits/42031
https://www.exploit-db.com/exploits/41987
https://www.exploit-db.com/exploits/41891