CVE Report: CVE-2017-0144

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.

Severity: HIGH | Score: 8.8

Exploit Links:

Date: 2019-10-02 | Platform: Windows | Author: Windows

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

Date: 2017-07-11 | Platform: Windows | Author: Windows

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

Date: 2017-05-17 | Platform: Windows_x86-64 | Author: Windows_x86-64

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

Date: 2017-05-17 | Platform: Windows | Author: Windows

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

Date: 2017-05-10 | Platform: Windows_x86-64 | Author: Windows_x86-64

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

Date: 2017-04-17 | Platform: Windows | Author: Windows

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

References:

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

http://packetstormsecurity.com/files/156196/SMB-DOUBLEPULSAR-Remote-Code-Execution.html

https://cert-portal.siemens.com/productcert/pdf/ssa-701903.pdf

https://cert-portal.siemens.com/productcert/pdf/ssa-966341.pdf

https://ics-cert.us-cert.gov/advisories/ICSMA-18-058-02

https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2017-0144

https://www.exploit-db.com/exploits/41891/

https://www.exploit-db.com/exploits/41987/

https://www.exploit-db.com/exploits/42030/

https://www.exploit-db.com/exploits/42031/