CVE Report

CVE ID: CVE-2017-0144

Score: 8.8

Severity: HIGH

CVSS Vector: CVSS:3.1/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.

confidentialityImpact: HIGH

integrityImpact: HIGH

availabilityImpact: HIGH

attackVector: NETWORK

Vendor: Microsoft Corporation

Product: Windows SMB

References: http://packetstormsecurity.com/files/154690/DOUBLEPULSAR-Payload-Execution-Neutralization.html, http://packetstormsecurity.com/files/156196/SMB-DOUBLEPULSAR-Remote-Code-Execution.html, 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/

State: PUBLISHED

# AI Response:

CVE-2017-0144Summary:Vulnerability Overview: CVE-2017-0144 is a vulnerability found in Microsoft Windows that affects the way the operating system handles font files. This flaw can be exploited by attackers to potentially gain control of a vulnerable system. It affects multiple Windows versions, including Windows 7, Windows 8.1, and Windows 10.In Simple Terms: Imagine your computer uses a special program to read font files. This program has a weakness that allows an attacker to trick it into running malicious code. If you open a specially crafted font file, the attacker could potentially take control of your computer without your knowledge.Potential Impact: If this vulnerability is exploited, an attacker could:Gain control of your computer: They could potentially run programs, view, change, or delete data, or create new accounts.  
Install malicious software: The attacker could install malware on your computer, which could steal your data, monitor your online activity, or harm your system.  
Spread malware to other computers: If your computer is connected to a network, the attacker could potentially spread malware to other devices on the network.Proactive Measures and Protection:Install security updates: Microsoft has released patches to address this vulnerability. Make sure you install the latest updates for your version of Windows.  
Be cautious with font files: Avoid opening font files from untrusted sources. If you receive a font file from an unknown sender, be wary before opening it.  
Use strong anti-virus software: A good anti-virus program can help protect your computer from malicious software, including malware that might be spread through font files.Broader Cybersecurity Context:Maintaining a strong cybersecurity posture is crucial. It's important to:Install updates regularly: This ensures your software is up-to-date with the latest security patches.  
Be wary of phishing attempts: Don't open suspicious emails or click on links from unknown sources.  
Use strong passwords and two-factor authentication: This makes it harder for attackers to access your accounts.Conclusion:CVE-2017-0144 is a serious vulnerability that could allow attackers to take control of your computer. By installing the latest updates for your Windows version and practicing good cybersecurity hygiene, you can significantly reduce your risk.