certin Handling Computer Security Incidents
Indian Computer Emergency Response Team
Ministry of Electronics and Information Technology
Government of India
सत्यमेव जयते

CERT-In Vulnerability Note CIVN-2017-0032
Multiple vulnerabilities in Windows SMB (CRITICAL)

Original Issue Date:March 15, 2017

Severity Rating: HIGH

Software Affected

- Windows Vista Service Pack 2 and Windows Vista x64 Edition Service Pack 2
- Windows 7 for 32-bit Service Pack 1 and Windows 7 for x64-based Systems Service Pack 1
- Windows 8.1 for 32-bit and 64-bit systems
- Windows RT 8.1
- Windows 10 for 32 bit and 64-bit systems
- Windows Server 2012
- Windows Server 2012 R2
- Windows Server 2008 R2 for x64-based Systems Service Pack 1
- Windows Server 2008 SP2 for 32-bit and 64-bit systems (Server Core Installation)
- Windows Server 2008 SP1 R2 for64-bit Systems(Server Core Installation)
- Windows Server 2008 R2 for Itanium-based Systems Service Pack 1
- Windows Server 2008 for Itanium-based Systems Service Pack 2
- Windows Server 2012 (Server Core Installation)
- Windows Server 2012 R2(Server Core Installation)
- Windows Server 2016 for 64-bit Systems(Server Core Installation)
- Windows Server 2016 for 64-bit Systems

Overview

Multiple remote code execution vulnerabilities and an Information Disclosure Vulnerability exist in the way that the Microsoft Server Message Block 1.0 (SMBv1) server handles certain requests which could be exploited by a remote attacker to execute code on the target server.

Note :- This vulnerability is being exploited by Wannacry / WannaCrypt Ransomware.

Description

1. Remote Code Execution Vulnerabilities (CVE-2017-0143 CVE-2017-0144 CVE-2017-0145 CVE-2017-0146 CVE-2017-0148)

These vulnerabilities exist in the way that the Microsoft Server Message Block 1.0 (SMBv1) server handles certain specially crafted requests. A unauthenticated attacker could exploit these vulnerabilities by sending specially crafted packets to the targeted SMBv1 server, which could lead him to run an arbitrary code.

2. Windows SMB Information Disclosure Vulnerability (CVE-2017-0147)

This vulnerability exists in the way that the Microsoft Server Message Block 1.0 (SMBv1) server handles certain specially crafted requests. A unauthenticated attacker could exploit this vulnerability by sending a specially crafted packet to a targeted SMBv1 server, which could lead to information disclosure from the server.

Solution

Apply appropriate patches as mentioned in Microsoft Security Bulletin MS17-010

Vendor Information

Microsoft
https://technet.microsoft.com/en-us/library/security/ms17-010.aspx

References

Microsoft
https://technet.microsoft.com/en-us/library/security/ms17-010.aspx

Cisco
https://tools.cisco.com/security/center/viewAlert.x?alertId=52834
https://tools.cisco.com/security/center/viewAlert.x?alertId=52838

CVE Name
CVE-2017-0143
CVE-2017-0144
CVE-2017-0145
CVE-2017-0146
CVE-2017-0147
CVE-2017-0148

Disclaimer

The information provided herein is on "as is" basis, without warranty of any kind.

Contact Information

Email: info@cert-in.org.in
Phone: +91-11-24368572

Postal address

Indian Computer Emergency Response Team (CERT-In)
Ministry of Electronics and Information Technology
Government of India
Electronics Niketan
6, CGO Complex, Lodhi Road,
New Delhi - 110 003
India