TLP: WHITE
MS-ISAC CYBERSECURITY ADVISORY

MS-ISAC ADVISORY NUMBER:
*2017-024 - **UPDATED***

DATE(S) ISSUED:
03/14/2017
05/12/2017 - UPDATED

SUBJECT:
Multiple Vulnerabilities in Microsoft Windows SMB Server Could Allow for Remote Code Execution (MS17-010)

OVERVIEW:
Multiple vulnerabilities have been discovered in Microsoft Windows SMB Server, the most severe of which could allow for remote code execution if an attacker sends specially crafted messages to a Microsoft Server Message Block 1.0 (SMBv1) server. Successful exploitation of the most severe of these vulnerabilities could result in an attacker gaining the same privileges as the logged on user. Depending on the privileges associated with the user, an attacker could then install programs; view, change, or delete data; or create new accounts with full user rights. Users whose accounts are configured to have fewer user rights on the system could be less impacted than those who operate with administrative user rights.

THREAT INTELLIGENCE:
There are currently no reports of these vulnerabilities being exploited in the wild.

May 12 – UPDATED THREAT INTELLIGENCE:
These vulnerabilities have recently been associated with exploitation from the WannaCry ransomware campaign. This activity has been observed impacting entities from various sectors as well as being on a global scale. The attack vector is unknown at this time but reports have indicated malvertising, exploit kits, and email spam as being a part of the infection vector. Please see the updated references section for open-source news regarding the ransomware activity.

SYSTEMS AFFECTED:
- Microsoft Windows: Vista, 7, 8.1, RT 8.1, 10
- Microsoft Windows Server: 2008, 2008 R2, 2012, 2012 R2, 2016
- Microsoft Windows Server Core Installations: 2008, 2008 R2, 2012, 2012 R2, 2016

RISK:
Government:
- Large and medium government entities: **High**
- Small government entities: **Medium**

Businesses:

- Large and medium business entities: **High**
- Small business entities: **Medium**

Home users: Low

TECHNICAL SUMMARY:

Multiple vulnerabilities have been identified in Microsoft Windows SMB Server, the most severe of which could allow for remote code execution. The vulnerabilities are as follows:

- Multiple remote code execution vulnerabilities exist due to the way the Microsoft Server Message Block 1.0 (SMBv1) server handles certain requests. (CVE-2017-0143, CVE-2017-0144, CVE-2017-0145, CVE-2017-0146, CVE-2017-148)
- An information disclosure vulnerability exists due to the way the Microsoft Server Message Block 1.0 (SMBv1) server handles certain requests memory. (CVE-2017-0147)

To exploit these vulnerabilities an unauthenticated attacker could send a specially crafted packet to a targeted SMBv1 server. Successful exploitation of the most severe of these vulnerabilities could result in an attacker gaining the same privileges as the logged on user. Depending on the privileges associated with the user, an attacker could then install programs; view, change, or delete data; or create new accounts with full user rights. Users whose accounts are configured to have fewer user rights on the system could be less impacted than those who operate with administrative user rights.

RECOMMENDATIONS:

We recommend the following actions be taken:

- Apply appropriate patches provided by Microsoft to vulnerable systems immediately after appropriate testing.
- Disable SMBv1 on all systems and utilize SMBv2 or SMBv3 after appropriate testing.
- Run all software as a non-privileged user (one without administrative privileges) to diminish the effects of a successful attack.
- Remind users not to visit un-trusted websites or follow links provided by unknown or un-trusted sources.
- Inform and educate users regarding the threats posed by hypertext links contained in emails or attachments, especially those from un-trusted sources.
- Apply the Principle of Least Privilege to all systems and services.

REFERENCES:

Microsoft:

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

CVE:

http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-0143
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-0144
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-0145

http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-0146
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-0147
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-0148

May 12 – UPDATED REFERENCES:

Open-Source News:
http://www.wired.co.uk/article/wanna-decryptor-ransomware
https://www.theregister.co.uk/2017/05/12/nhs_hospital_shut_down_due_to_cyber_attack/

24×7 Security Operations Center
Multi-State Information Sharing and Analysis Center (MS-ISAC)
31 Tech Valley Drive
East Greenbush, NY 12061
SOC@cisecurity.org - 1-866-787-4722