SAINT Patch Report Sample

Report Generated: December 2, 2015

1 Introduction

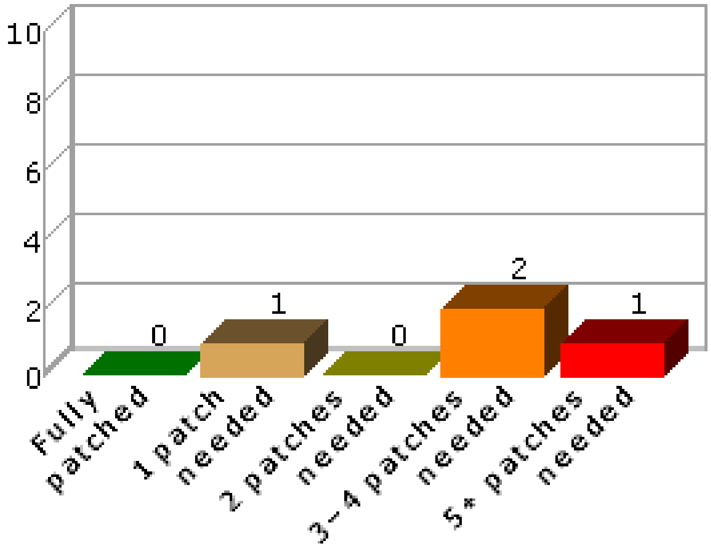
On December 2, 2015, at 12:58 PM, a heavy vulnerability assessment was conducted using the SAINT 8.9.24 vulnerability scanner. The scan discovered a total of four live hosts, and detected 15 needed patches affecting four hosts. The hosts and problems detected are discussed in greater detail in the following sections.

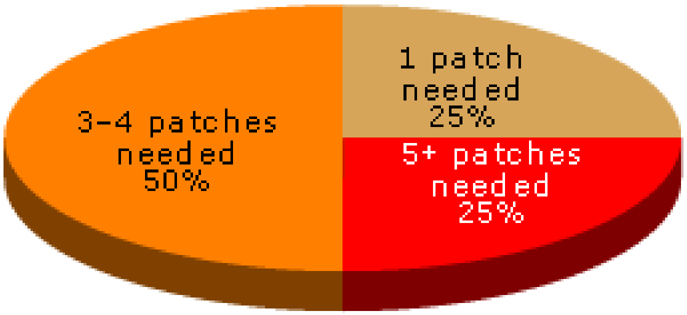
2 Summary

The sections below summarize the results of the scan.

2.1 Hosts by Needed Patches

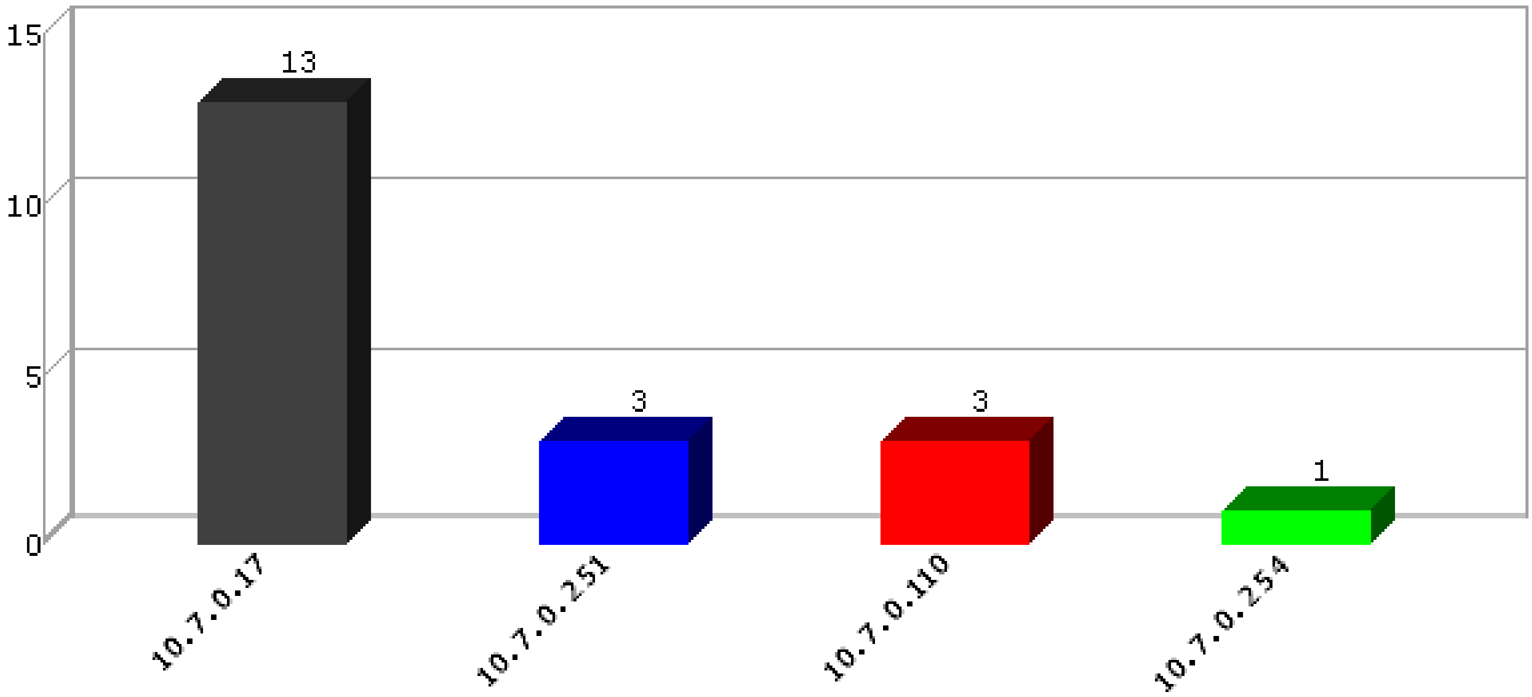
This section shows the number of hosts detected with various numbers of missing patches.





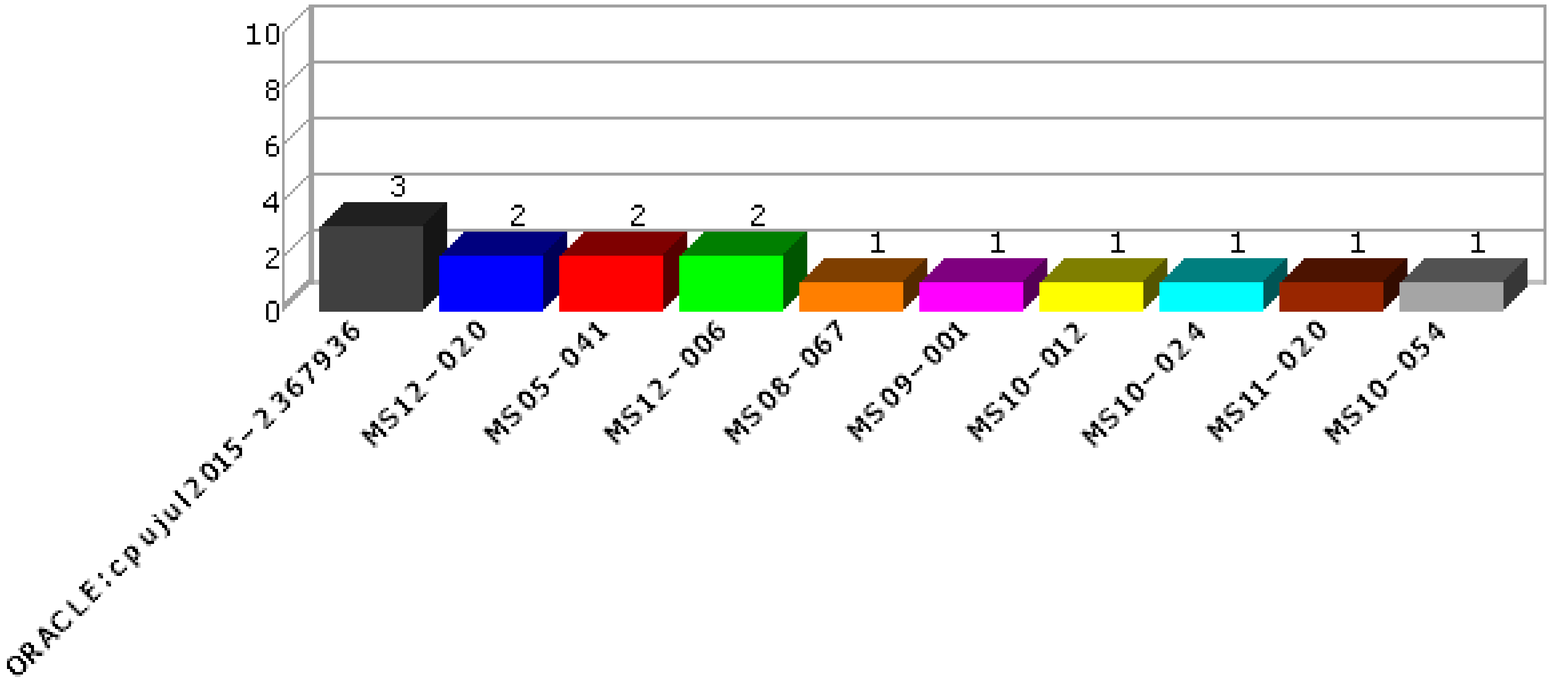
2.2 Top 10 Vulnerable Hosts

This section shows the most vulnerable hosts detected, and the number of missing patches detected on them.



2.3 Top 10 Patches

This section shows the most commonly detected missing patches, and the number of hosts on which they are needed.



3 Overview

The following tables present an overview of the hosts discovered on the network and the vulnerabilities contained therein.

3.1 Host List

This table presents an overview of the hosts discovered on the network.

Host Name	Netbios Name	IP Address	Host Type	Patches Needed
10.7.0.17	RELEASE_WIN2003	10.7.0.17	Windows Server 2003 SP1	13
10.7.0.110	WIN10	10.7.0.110	Windows 10	3
10.7.0.251		10.7.0.251	Windows Server 2008 R2 SP1	3
10.7.0.254		10.7.0.254	Cisco IOS 11.3	1

4 Patch Details

The following sections provide details of missing patches detected on the network.

4.1 MS12-020

https://technet.microsoft.com/library/security/MS12-020

Host name: 10.7.0.17 **IP Address:** 10.7.0.17

- Microsoft Remote Desktop Protocol Remote Code Execution Vulnerability (MS12-020)

Host name: 10.7.0.251 **IP Address:** 10.7.0.251

- Microsoft Remote Desktop Protocol Remote Code Execution Vulnerability (MS12-020)

4.2 MS08-067

https://technet.microsoft.com/library/security/MS08-067

Host name: 10.7.0.17 **IP Address:** 10.7.0.17

- Windows Server Service MS08-067 buffer overflow

4.3 MS09-001

https://technet.microsoft.com/library/security/MS09-001

Host name: 10.7.0.17 **IP Address:** 10.7.0.17

- Multiple buffer overflows in SMB

4.4 MS10-012

https://technet.microsoft.com/library/security/MS10-012

Host name: 10.7.0.17	**IP Address:** 10.7.0.17

- vulnerable version of SMB Server (MS10-012)

4.5 MS10-024

https://technet.microsoft.com/library/security/MS10-024

Host name: 10.7.0.17	**IP Address:** 10.7.0.17

- vulnerable Microsoft mail server version: 6.0.3790.1830

4.6 MS11-020

https://technet.microsoft.com/library/security/MS11-020

Host name: 10.7.0.17	**IP Address:** 10.7.0.17

- Windows SMB Server Transaction Vulnerability

4.7 MS10-054

https://technet.microsoft.com/library/security/MS10-054

Host name: 10.7.0.17	**IP Address:** 10.7.0.17

- Over-the-network SMB packet vulnerabilities in Windows system (MS10-054)

4.8 MS15-011

https://technet.microsoft.com/library/security/MS15-011

Host name: 10.7.0.17	**IP Address:** 10.7.0.17

- Group Policy Code Execution Vulnerability (MS15-011)

4.9 ORACLE:cpujul2015-2367936

http://www.oracle.com/technetwork/topics/security/cpujul2015-2367936.html

Host name: 10.7.0.110	**IP Address:** 10.7.0.110

- SSL/TLS server supports RC4 ciphers

Host name: 10.7.0.251 **IP Address:** 10.7.0.251

- SSL/TLS server supports RC4 ciphers

Host name: 10.7.0.254 **IP Address:** 10.7.0.254

- SSL/TLS server supports RC4 ciphers

4.10 MS05-041

https://technet.microsoft.com/library/security/MS05-041

Host name: 10.7.0.110 **IP Address:** 10.7.0.110

- Possible vulnerability in Microsoft Terminal Server

Host name: 10.7.0.17 **IP Address:** 10.7.0.17

- Possible vulnerability in Microsoft Terminal Server

4.11 MS12-006

https://technet.microsoft.com/library/security/MS12-006

Host name: 10.7.0.110 **IP Address:** 10.7.0.110

- server is susceptible to BEAST attack

Host name: 10.7.0.251 **IP Address:** 10.7.0.251

- server is susceptible to BEAST attack

4.12 MS06-003

https://technet.microsoft.com/library/security/MS06-003

Host name: 10.7.0.17 **IP Address:** 10.7.0.17

- possible Microsoft Exchange Buffer overflow in TNEF encoded messages

4.13 MS06-034

https://technet.microsoft.com/library/security/MS06-034

Host name: 10.7.0.17 **IP Address:** 10.7.0.17

- Possible Microsoft IIS ASP Upload Command Execution vulnerability

4.14 MS09-053

https://technet.microsoft.com/library/security/MS09-053

Host name: 10.7.0.17	**IP Address:** 10.7.0.17

- Microsoft Internet Information Services FTP Server Remote Buffer Overflow

4.15 Sendmail 8.9

http://www.sendmail.org

Host name: 10.7.0.17	**IP Address:** 10.7.0.17

- SMTP may be a mail relay

Scan Session: Uncredentialed subnet scan; Scan Policy: heavy vulnerability; Scan Data Set: 2 December 2015 12:58