SAINTwriter Assessment Report

Report Generated: May 4, 2011

1.0 Introduction

This is a sample report that provides an illustration of vulnerabilities and the number of affected systems by each vulnerability.

2.0 Details

The following sections provide details of various hosts for each vulnerability.

2.1 Routing and Remote Access Service remote code execution

Host name: 10.7.0.2
Host type: Windows 2000 SP2
Scan time: May 03 23:28:33 2011
Severity: Critical Problem

IP Address: 10.7.0.2
Netbios name: SAINTLAB02

CVE: CVE-2006-2370 CVE-2006-2371

Host name: 10.7.0.11
Host type: Windows Server 2003 SP1
Scan time: May 03 23:34:29 2011
Severity: Critical Problem

IP Address: 10.7.0.11
Netbios name: WIN2003UNPATCH

CVE: CVE-2006-2370 CVE-2006-2371

Technical Details

Service: netbios
Remote Access Connection Manager service running and KB911280 not installed

2.2 Windows Server Service MS08-067 buffer overflow

Host name: 10.7.0.2
Host type: Windows 2000 SP2
Scan time: May 03 23:28:33 2011
Severity: Critical Problem

IP Address: 10.7.0.2
Netbios name: SAINTLAB02

CVE: CVE-2008-4250

Host name: 10.7.0.15
Host type: Windows 2000 SP2
Scan time: May 03 23:36:18 2011
Severity: Critical Problem

IP Address: 10.7.0.15
Netbios name: TRAINING2

CVE: CVE-2008-4250

Host name: 10.7.0.14
Host type: Windows XP SP2
Scan time: May 03 23:28:33 2011
Severity: Critical Problem

IP Address: 10.7.0.14
Netbios name: XPPROUNPATCHED

CVE: CVE-2008-4250

Host name: 10.7.0.11
Host type: Windows Server 2003 SP1
Scan time: May 03 23:34:29 2011
Severity: Critical Problem

IP Address: 10.7.0.11
Netbios name: WIN2003UNPATCH

CVE: CVE-2008-4250

Technical Details

Service: 445:TCP
NetprPathCompare returned 0

2.3 Windows print spooler vulnerabilities

Host name: 10.7.0.2
Host type: Windows 2000 SP2
Scan time: May 03 23:28:33 2011
Severity: Critical Problem

IP Address: 10.7.0.2
Netbios name: SAINTLAB02

CVE: CVE-2009-0228 CVE-2009-0229 CVE-2009-0230

Host name: 10.7.0.15
Host type: Windows 2000 SP2
Scan time: May 03 23:36:18 2011
Severity: Critical Problem

IP Address: 10.7.0.15
Netbios name: TRAINING2

CVE: CVE-2009-0228 CVE-2009-0229 CVE-2009-0230

Host name: 10.7.0.14
Host type: Windows XP SP2
Scan time: May 03 23:28:33 2011
Severity: Area of Concern

IP Address: 10.7.0.14
Netbios name: XPPROUNPATCHED

CVE: CVE-2009-0228 CVE-2009-0229 CVE-2009-0230

Host name: 10.7.0.11
Host type: Windows Server 2003 SP1
Scan time: May 03 23:34:29 2011
Severity: Area of Concern

IP Address: 10.7.0.11
Netbios name: WIN2003UNPATCH

CVE: CVE-2009-0228 CVE-2009-0229 CVE-2009-0230

Technical Details

Service: netbios
SOFTWARE\Microsoft\Updates\Windows Server 2003\SP3\KB961501 not found

2.4 Windows Message Queuing validation vulnerability

Host name: 10.7.0.2
Host type: Windows 2000 SP2
Scan time: May 03 23:28:33 2011
Severity: Critical Problem

IP Address: 10.7.0.2
Netbios name: SAINTLAB02

CVE: CVE-2007-3039

Host name: 10.7.0.14
Host type: Windows XP SP2
Scan time: May 03 23:28:33 2011

IP Address: 10.7.0.14
Netbios name: XPPROUNPATCHED

Severity: Area of Concern **CVE:** CVE-2007-3039

Technical Details

Service: netbios
mqutil.dll older than 2007-7-4

2.5 Windows Server Service Buffer Overrun

Host name: 10.7.0.2 **IP Address:** 10.7.0.2
Host type: Windows 2000 SP2 **Netbios name:** SAINTLAB02
Scan time: May 03 23:28:33 2011
Severity: Critical Problem **CVE:** CVE-2006-3439

Host name: 10.7.0.14 **IP Address:** 10.7.0.14
Host type: Windows XP SP2 **Netbios name:** XPPROUNPATCHED
Scan time: May 03 23:28:33 2011
Severity: Critical Problem **CVE:** CVE-2006-3439

Technical Details

Service: 445:TCP
Sent netrpPathCanonicalize call, response indicates patch not applied

2.6 Windows Workstation service remote code execution

Host name: 10.7.0.2 **IP Address:** 10.7.0.2
Host type: Windows 2000 SP2 **Netbios name:** SAINTLAB02
Scan time: May 03 23:28:33 2011
Severity: Critical Problem **CVE:** CVE-2006-4691

Host name: 10.7.0.15 **IP Address:** 10.7.0.15
Host type: Windows 2000 SP2 **Netbios name:** TRAINING2
Scan time: May 03 23:36:18 2011
Severity: Critical Problem **CVE:** CVE-2006-4691

Host name: 10.7.0.14 **IP Address:** 10.7.0.14
Host type: Windows XP SP2 **Netbios name:** XPPROUNPATCHED
Scan time: May 03 23:28:33 2011
Severity: Area of Concern **CVE:** CVE-2006-4691

Technical Details

Service: netbios
SOFTWARE\Microsoft\Updates\Windows XP\SP3\KB924270 not found

2.7 Windows WMF gdi32.dll vulnerability

Host name: 10.7.0.2 **IP Address:** 10.7.0.2
Host type: Windows 2000 SP2 **Netbios name:** SAINTLAB02
Scan time: May 03 23:28:33 2011
Severity: Critical Problem **CVE:** CVE-2005-4560

Host name: 10.7.0.15
Host type: Windows 2000 SP2
Scan time: May 03 23:36:18 2011
Severity: Critical Problem

IP Address: 10.7.0.15
Netbios name: TRAINING2

CVE: CVE-2005-4560

Technical Details

Service: netbios
gdi32.dll older than 2005-12-25

2.8 Windows 2000 RPC buffer overflow

Host name: 10.7.0.2
Host type: Windows 2000 SP2
Scan time: May 03 23:28:33 2011
Severity: Critical Problem

IP Address: 10.7.0.2
Netbios name: SAINTLAB02

CVE: CVE-2003-0352

Technical Details

Service: netbios
SOFTWARE\Microsoft\Updates\Windows 2000\SP5\KB823980 not found

2.9 Telnet

Host name: 10.7.0.5
Host type: SunOS 5.6
Scan time: May 03 23:28:36 2011
Severity: Service

IP Address: 10.7.0.5

Host name: 10.7.0.4
Host type: FreeBSD
Scan time: May 03 23:28:36 2011
Severity: Service

IP Address: 10.7.0.4

Technical Details

\000

Scan Session: 10.7 Exploit Only; Scan Policy: custom; Scan Data Set: 3 May 2011 23:36