



Report

Scan Result

Ports	Service	Version	State
22/tcp	ssh	OpenSSH 4.7p1 Debian 8ubuntu1	open
23/tcp	telnet	Linux telnetd	open
25/tcp	smtp	Postfix smtpd	open
53/tcp	domain	ISC BIND 9.4.2	open
80/tcp	http	Apache httpd 2.2.8	open
111/tcp	rpcbind		open
139/tcp	netbios-ssn	Samba smbd 3.X - 4.X	open
445/tcp	netbios-ssn	Samba smbd 3.X - 4.X	open
512/tcp	exec		open
513/tcp	login	OpenBSD or Solaris rlogind	open
514/tcp	tcpwrapped		open

OS Detection

Name	Accuracy
Linux 2.6.9 - 2.6.33	100

CVE Result

service	ISC BIND 9.4.2
id	CVE-2008-0122
description	Off-by-one error in the inet_network function in libbind in ISC BIND 9.4.2 and earlier, as used in libc in FreeBSD 6.2 through 7.0-PRERELEASE, allows context-dependent attackers to cause a denial of service (crash) and possibly execute arbitrary code via crafted input that triggers memory corruption.
resource	http://lists.opensuse.org/opensuse-security-announce/2008-03/msg00004.html
id	CVE-2008-1447
description	The DNS protocol, as implemented in (1) BIND 8 and 9 before 9.5.0-P1, 9.4.2-P1, and 9.3.5-P1; (2)

Microsoft DNS in Windows 2000 SP4, XP SP2 and SP3, and Server 2003 SP1 and SP2; and other implementations allow remote attackers to spoof DNS traffic via a birthday attack that uses in-bailiwick referrals to conduct cache poisoning against recursive resolvers, related to insufficient randomness of DNS transaction IDs and source ports, aka "DNS Insufficient Socket Entropy Vulnerability" or "the Kaminsky bug."

resource	ftp://ftp.netbsd.org/pub/NetBSD/security/advisories/NetBSD-SA2008-009.txt.asc
id	CVE-2008-4163
description	Unspecified vulnerability in ISC BIND 9.3.5-P2-W1, 9.4.2-P2-W1, and 9.5.0-P2-W1 on Windows allows remote attackers to cause a denial of service (UDP client handler termination) via unknown vectors.
resource	http://marc.info/?l=bind-announce&m=122180244228376&w=2

service	vsftpd 2.3.4
id	CVE-2011-0762
description	<p>The vsf_filename_passes_filter function in ls.c in vsftpd before 2.3.3 allows remote authenticated users to cause a denial of service (CPU consumption and process slot exhaustion) via crafted glob expressions in STAT commands in multiple FTP sessions, a different vulnerability than CVE-2010-2632.</p>
resource	<p>ftp://vsftpd.beasts.org/users/cevans/untar/vsftpd-2.3.4/Changelog</p>
id	CVE-2011-2523
description	<p>vsftpd 2.3.4 downloaded between 20110630 and 20110703 contains a backdoor which opens a shell on port 6200/tcp.</p>
resource	<p>http://packetstormsecurity.com/files/162145/vsftpd-2.3.4-Backdoor-Command-Execution.html</p>
service	OpenSSH 4.7p1 Debian 8ubuntu1