CVE-2008-1447

MITRE | NVD | CVE.ORG | JSON API | Print: PDF

Summary

CVE	CVE-2008-1447
State	PUBLIC
Assigner	secure@microsoft.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2008-07-08 23:41:00 UTC
Updated	2020-03-24 18:19:00 UTC
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 Wind

Risk And Classification

Problem Types: CWE-331

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Canonical	Ubuntu Linux	6.06	All	All	All
Operating System	Canonical	Ubuntu Linux	7.04	All	All	All
Operating System	Canonical	Ubuntu Linux	7.10	All	All	All
Operating System	Canonical	Ubuntu Linux	8.04	All	All	All
Operating System	Canonical	Ubuntu Linux	6.06	All	All	All
Operating System	Canonical	Ubuntu Linux	7.04	All	All	All
Operating System	Canonical	Ubuntu Linux	7.10	All	All	All
Operating System	Canonical	Ubuntu Linux	8.04	All	All	All
Operating System	Cisco	Ios	12.0	All	All	All
Operating System	Cisco	Ios	12.0	All	All	All
Operating System	Debian	Debian Linux	4.0	All	All	All
Operating System	Debian	Debian Linux	4.0	All	All	All
Application	Isc	Bind	4	All	All	All
Application	Isc	Bind	8	All	All	All
Application	Isc	Bind	9.2.9	All	All	All
Application	Isc	Bind	4	All	All	All
Application	Isc	Bind	8	All	All	All

Application	Isc	Bind	9.2.9	All	All	All
Operating System	Microsoft	Windows 2000	All	sp4	All	All
Operating System	Microsoft	Windows 2000	All	sp4	All	All
Operating System	Microsoft	Windows Server 2003	-	All	All	All
Operating System	Microsoft	Windows Server 2003	-	sp1	All	All
Operating System	Microsoft	Windows Server 2003	-	sp1	All	All
Operating System	Microsoft	Windows Server 2003	-	sp1	All	All
Operating System	Microsoft	Windows Server 2003	-	sp1	All	All
Operating System	Microsoft	Windows Server 2003	-	sp1	All	All
Operating System	Microsoft	Windows Server 2003	-	sp2	All	All
Operating System	Microsoft	Windows Server 2003	-	sp2	All	All
Operating System	Microsoft	Windows Server 2003	-	sp2	All	All
Operating System	Microsoft	Windows Server 2003	-	sp2	All	All
Operating System	Microsoft	Windows Server 2003	-	sp2	All	All
Operating System	Microsoft	Windows Server 2003	-	sp2	All	All
Operating System	Microsoft	Windows Server 2003	-	sp2	All	All
Operating System	Microsoft	Windows Server 2003	-	sp2	All	All
Operating System	Microsoft	Windows Server 2003	-	sp2	All	All
Operating System	Microsoft	Windows Server 2003	-	sp2	All	All
Operating System	Microsoft	Windows Server 2003	-	All	All	All
Operating System	Microsoft	Windows Server 2003	-	sp1	All	All
Operating System	Microsoft	Windows Server 2003	-	sp1	All	All
Operating System	Microsoft	Windows Server 2003	-	sp1	All	All
Operating System	Microsoft	Windows Server 2003	-	sp1	All	All
Operating System	Microsoft	Windows Server 2003	-	sp1	All	All
Operating System	Microsoft	Windows Server 2003	-	sp2	All	All
Operating System	Microsoft	Windows Server 2003	-	sp2	All	All
Operating System	Microsoft	Windows Server 2003	-	sp2	All	All
Operating System	Microsoft	Windows Server 2003	-	sp2	All	All
Operating System	Microsoft	Windows Server 2003	-	sp2	All	All
Operating System	Microsoft	Windows Server 2003	-	sp2	All	All
Operating System	Microsoft	Windows Server 2003	-	sp2	All	All
Operating System	Microsoft	Windows Server 2003	-	sp2	All	All
Operating System	Microsoft	Windows Server 2003	-	sp2	All	All
Operating System	Microsoft	Windows Server 2003	-	sp2	All	All

Operating System	Microsoft	Windows Xp	All	sp2	All	All
Operating System	Microsoft	Windows Xp	-	-	All	All
Operating System	Microsoft	Windows Xp	-	sp3	All	All
Operating System	Microsoft	Windows Xp	All	sp2	All	All
Operating System	Microsoft	Windows Xp	-	-	All	All
Operating System	Microsoft	Windows Xp	-	sp3	All	All
Operating System	Redhat	Enterprise Linux	2.1	All	as	All
Operating System	Redhat	Enterprise Linux	2.1	All	es	All
Operating System	Redhat	Enterprise Linux	2.1	All	ws	All
Operating System	Redhat	Enterprise Linux	5	All	client	All
Operating System	Redhat	Enterprise Linux	5	All	client_workstation	All
Operating System	Redhat	Enterprise Linux	5.0	All	All	All
Operating System	Redhat	Enterprise Linux	2.1	All	as	All
Operating System	Redhat	Enterprise Linux	2.1	All	es	All
Operating System	Redhat	Enterprise Linux	2.1	All	ws	All
Operating System	Redhat	Enterprise Linux	5	All	client	All
Operating System	Redhat	Enterprise Linux	5	All	client_workstation	All
Operating System	Redhat	Enterprise Linux	5.0	All	All	All

References

Reference
SSRT080058
Webmail - OVH
Webmail - OVH
Webmail - OVH
IBM IZ26672: POTENTIAL SECURITY ISSUE IN BIND CVE-2008-1447 APPLIES TO AIX 6100-01 - United States
About the security content of iPhone v2.1
Webmail - OVH
Webmail : Solution de messagerie professionnelle - OVHcloud- OVH
BIND: Cache poisoning — Gentoo Linux Documentation
US-CERT Technical Cyber Security Alert TA08-190A -- Microsoft Updates for Multiple Vulnerabilities
Dnsmasq DNS Query Port Entropy Weakness Lets Remote Users Spoof the System - SecurityTracker
Cisco Security Advisory: Multiple Cisco Products Vulnerable to DNS Cache Poisoning Attacks [Products & Services] - Cisco Systems
HP Tru64 UNIX BIND Query Port DNS Cache Poisoning - Secunia.com
rhn.redhat.com | Red Hat Support
Webmail - OVH

FreeBSD-SA-08:06

Blue Coat ProxyRA DNS Cache Poisoning Vulnerability - Secunia Advisories - Vulnerability Information - Secunia.com

IBM IZ26670: POTENTIAL SECURITY ISSUE IN BIND CVE-2008-1447 APPLIES TO AIX 5300-08 - United States

Webmail - OVH

HPSBNS02405

OpenBSD BIND Query Port DNS Cache Poisoning - Secunia Advisories - Vulnerability Intelligence - Secunia.com

Fedora update for bind - Secunia Advisories - Vulnerability Intelligence - Secunia.com

Ruby Multiple Vulnerabilities - Secunia Advisories - Vulnerability Intelligence - Secunia.com

Debian -- Security Information -- DSA-1619-1 python-dns

Debian update for python-dns - Secunia Advisories - Vulnerability Intelligence - Secunia.com

Webmail - OVH

Multiple Vendor DNS Protocol Insufficient Transaction ID Randomization DNS Spoofing Vulnerability

APPLE-SA-2008-09-15 Mac OS X v10.5.5 and Security Update 2008-006

NetBSD update for bind - Advisories - Secunia

SUSE Update for Multiple Packages - Secunia Advisories - Vulnerability Intelligence - Secunia.com

Webmail - OVH

Ubuntu update for bind - Secunia Advisories - Vulnerability Intelligence - Secunia.com

www.caughq.org/exploits/CAU-EX-2008-0003.txt

[security-announce] SUSE Security Summary Report SUSE-SR:2008:017

IPCop update for various packages - Secunia Advisories - Vulnerability Intelligence - Secunia.com

Webmail : Solution de messagerie professionnelle - OVHcloud- OVH

Support

Webmail : Solution de messagerie professionnelle - OVHcloud- OVH

IBM notice: The page you requested cannot be displayed

Repository / Oval Repository

Gentoo Linux Documentation -- VMware Player, Server, Workstation: Multiple vulnerabilities

Nortel: Technical Support: Nortel Guidance for Multiple Vendor Fixes for BIND/DNS Cache Poison Vulnerability - CVE-2008-1447

Webmail - OVH

Infoblox Information for VU#800113

Apple Mac OS X Security Update Fixes Multiple Vulnerabilities - Secunia Advisories - Vulnerability Intelligence - Secunia.com

Webmail - OVH

Cisco Firewall Service Module Predictable Source Port Address Translation Leaves DNS Servers Vulnerable to Recent Cache Poisoning Atta

Invisible Denizen: Kaminsky's DNS Issue Accidentally Leaked?

Webmail - OVH

USN-622-1: Bind vulnerability | Ubuntu

[security-announce] SUSE Security Announcement: bind (SUSE-SA:2008:033)

IBM IZ26668: POTENTIAL SECURITY ISSUE IN BIND CVE-2008-1447 APPLIES TO AIX 5300-06 - United States

[Full-disclosure] VMSA-2008-0014 Updates to VMware Workstation, VMware Player, VMware ACE, VMware Server, VMware ESX address in

Debian -- Security Information -- DSA-1605-1 glibc

Juniper JUNOS DNS Query Port Entropy Weakness Lets Remote Users Spoof the System - SecurityTracker

IBM X-Force Exchange

SecurityTracker.com Archives - BIND DNS Query Port Entropy Weakness Lets Remote Users Spoof the System

Microsoft Security Bulletin MS08-037 - Important | Microsoft Docs

HP TCP/IP Services for OpenVMS BIND DNS Cache Poisoning - Secunia.com

FreeBSD update for bind - Secunia Advisories - Vulnerability Intelligence - Secunia.com

Webmail : Solution de messagerie professionnelle - OVHcloud- OVH

APPLE-SA-2008-09-12 iPhone v2.1

VitalQIP Query Port Entropy Weakness Lets Remote Users Spoof the System - SecurityTracker

BIND 9.4.1-9.4.2 Remote DNS Cache Poisoning Flaw Exploit (meta)

Debian update for dnsmasq - Secunia Advisories - Vulnerability Intelligence - Secunia.com

IPCop 1.4.19 / 1.4.20 released :: IPCop.org :: The bad packets stop here!

Sun Solaris 10 DNS Cache Poisoning Vulnerability - Secunia Advisories - Vulnerability Intelligence - Secunia.com

Blue Coat Director DNS Cache Poisoning Vulnerability - Advisories - Secunia

Webmail - OVH

Red Hat update for dnsmasq - Secunia Advisories - Vulnerability Intelligence - Secunia.com

F5 Products DNS Cache Poisoning Vulnerability - Advisories - Secunia

SecurityFocus

Webmail - OVH

Webmail : Solution de messagerie professionnelle - OVHcloud- OVH

Juniper Networks Products DNS Cache Poisoning Vulnerability - Secunia Advisories - Vulnerability Intelligence - Secunia.com

Debian -- Security Information -- DSA-1603-1 bind9

BlueCat Networks Adonis DNS Cache Poisoning - Secunia Advisories - Vulnerability Intelligence - Secunia.com

Microsoft Windows DNS Spoofing Vulnerabilities - Secunia Advisories - Vulnerability Intelligence - Secunia.com

US-CERT Vulnerability Note VU#800113

Cisco IOS Predictable Source Port Address Translation May Leave DNS Servers Vulnerable to Recent Cache Poisoning Attack - SecurityTrac

Advisories:rPSA-2010-0018 - rPath Wiki

About Secunia Research | Flexera

Webmail - OVH

#494401 - ruby1.8: New release (1.8.7-p71) with vulnerabilities fixes - Debian Bug report logs

Webmail - OVH

APPLE-SA-2008-07-31 Security Update 2008-005

APPLE-SA-2008-07-31 Security Update 2008-005

HPSBOV02357

Citrix NetScaler DNS Cache Poisoning - Secunia Advisories - Vulnerability Intelligence - Secunia.com

Blue Coat ProxySG DNS Query Port Entropy Weakness Lets Remote Users Spoof the System - SecurityTracker

Webmail - OVH

Adonis DNS Query Port Entropy Weakness Lets Remote Users Spoof the System - SecurityTracker

Debian update for bind9 - Secunia Advisories - Vulnerability Intelligence - Secunia.com

Gentoo update for bind - Advisories - Secunia

APPLE-SA-2008-09-09 iPod touch v2.1

Vulnerability in Access Gateway Standard and Advanced Edition Appliance firmware could result in DNS Cache Poisoning

HP NonStop Server DNS Cache Poisoning Vulnerability - Secunia Advisories - Vulnerability Intelligence - Secunia.com

Repository / Oval Repository

Webmail - OVH

Webmail - OVH

13>0 : DoxPara Research

Cisco Content Switching Module Predictable Source Port Address Translation Leaves DNS Servers Vulnerable to Recent Cache Poisoning At

Support | Status of CVE-2008-1447 - Multiple DNS implementations vulnerable to cache poisoning

Repository / Oval Repository

OpenBSD 4.2 errata

Page not found | Dan Kaminsky's Blog

Advisories:rPSA-2008-0231 - rPath Wiki

Windows DNS Service Bugs Let Remote Users Spoof the System - SecurityTracker

OpenBSD 4.3 errata

ISC has a new website | Internet Systems Consortium

Red Hat update for bind - Secunia Advisories - Vulnerability Intelligence - Secunia.com

Webmail - OVH

Cisco PIX Firewall Predictable Source Port Address Translation Leaves DNS Servers Vulnerable to Recent Cache Poisoning Attack - Security

IBM IZ26671: POTENTIAL SECURITY ISSUE IN BIND CVE-2008-1447 APPLIES TO AIX 6100-00 - United States

Secure Computing Sidewinder DNS Query Port Entropy Weakness Lets Remote Users Spoof the System - SecurityTracker

IBM AIX DNS Cache Poisoning - Secunia Advisories - Vulnerability Intelligence - Secunia.com

Slackware update for bind - Advisories - Secunia

Astaro Security Gateway DNS Cache Poisoning - Secunia Advisories - Vulnerability Intelligence - Secunia.com

VMSA-2008-0014.3 - VMware

About the security content of iPod touch v2.1

US-CERT Technical Cyber Security Alert TA08-260A -- Apple Updates for Multiple Vulnerabilities

Blue Coat PacketShaper and iShaper DNS Cache Poisoning - Advisories - Secunia

Webmail - OVH

Nixu Secure Name Server BIND Query Port DNS Cache Poisoning - Secunia Advisories - Vulnerability Intelligence - Secunia.com

Juniper ScreenOS DNS Query Port Entropy Weakness Lets Remote Users Spoof the System - SecurityTracker

Webmail - OVH

The Slackware Linux Project: Slackware Security Advisories

Sidewinder and CyberGuard DNS Cache Poisoning - Secunia Advisories - Vulnerability Intelligence - Secunia.com

240048

US-CERT Technical Cyber Security Alert TA08-190B -- Multiple DNS implementations vulnerable to cache poisoning

Cisco ASA Predictable Source Port Address Translation Leaves DNS Servers Vulnerable to Recent Cache Poisoning Attack - SecurityTracker

Up2Date Announcements: Up2Date 7.202 released

www.nominum.com/asset_upload_file741_2661.pdf

Webmail : Solution de messagerie professionnelle - OVHcloud- OVH

www.caughq.org/exploits/CAU-EX-2008-0002.txt

dnsmasq Denial of Service and DNS Cache Poisoning - Secunia Advisories - Vulnerability Intelligence - Secunia.com

Ruby: Multiple vulnerabilities — Gentoo Linux Documentation

Yamaha RT Series Routers DNS Cache Poisoning - Secunia.com

HP MPE/iX DNS Cache Poisoning Vulnerability - Advisories - Community

HP-UX update for bind - Advisories - Secunia

Nortel Business Communications Manager DNS Query Port Entropy Weakness Lets Remote Users Spoof the System - SecurityTracker

Apple iPod Touch Multiple Vulnerabilities - Secunia Advisories - Vulnerability Intelligence - Secunia.com

Nortel Business Communications Manager BIND DNS Cache Poisoning - Secunia.com

Departement Natuurkunde - Universiteit Utrecht

Citrix Access Gateway DNS Query Port Entropy Weakness Lets Remote Users Spoof the System - SecurityTracker

BIND 9.x Remote DNS Cache Poisoning Flaw Exploit (c)

Apple iPhone Multiple Vulnerabilities - Secunia Advisories - Vulnerability Intelligence - Secunia.com

Debian -- Security Information -- DSA-1604-1 bind

Repository / Oval Repository

Webmail - OVH

IBM IZ26669: POTENTIAL SECURITY ISSUE IN BIND CVE-2008-1447 APPLIES TO AIX 5300-07 - United States

Cisco Products DNS Cache Poisoning Vulnerability - Secunia Advisories - Vulnerability Intelligence - Secunia.com

Webmail - OVH

FAQ for YAMAHA RT Series / Security

HPSBMP02404

Webmail - OVH

Debian -- Security Information -- DSA-1623-1 dnsmasq

Webmail - OVH

BIND 9.x Remote DNS Cache Poisoning Flaw Exploit (py)

Citrix NetScaler DNS Query Port Entropy Weakness Lets Remote Users Spoof the System - SecurityTracker

Infoblox NIOS BIND Query Port DNS Cache Poisoning - Secunia Advisories - Vulnerability Intelligence - Secunia.com

rPath update for bind - Secunia Advisories - Vulnerability Intelligence - Secunia.com

IBM X-Force Exchange

Ruby 'resolv.rb' DNS Query Port Entropy Weakness Lets Remote Users Spoof the System - SecurityTracker

Repository / Oval Repository

Novell Netware DNS Cache Poisoning Vulnerability - Secunia Advisories - Vulnerability Intelligence - Secunia.com

Webmail - OVH

[SECURITY] Fedora 9 Update: bind-9.5.0-33.P1.fc9

pdnsd maintenance page by Paul Rombouts

SUSE update for bind - Secunia Advisories - Vulnerability Intelligence - Secunia.com

'[security bulletin] HPSBOV03226 rev.1 - HP TCP/IP Services for OpenVMS, BIND 9 Resolver, Multiple Re' - MARC

Webmail - OVH

Multiple vulnerabilities in Ruby

Apple Mac OS X Security Update Fixes Multiple Vulnerabilities - Secunia Advisories - Vulnerability Intelligence - Secunia.com

USN-627-1: Dnsmasq vulnerability | Ubuntu

Broadcom Inc. | Connecting Everything

An Illustrated Guide to the Kaminsky DNS Vulnerability

CTX117991 - Vulnerability in NetScaler and Access Gateway Enterprise Edition could result in DNS Cache Poisoning - Citrix Knowledge Cent

Sun Solaris DNS Cache Poisoning Vulnerability - Secunia Advisories - Vulnerability Intelligence - Secunia.com

Webmail - OVH

SecurityFocus

Ubuntu update for dnsmasq - Advisories - Secunia

Webmail - OVH

HPSBTU02358

#239392: Security Vulnerability in the DNS Protocol may lead to DNS Cache Poisoning

Webmail - OVH

Support / Security / Advisories / / MDVSA-2008:139 | Mandriva

SecurityTracker.com Archives - Cisco IOS DNS Query Port Entropy Weakness Lets Remote Users Spoof the System

Slackware update for dnsmasq - Secunia Advisories - Vulnerability Intelligence - Secunia.com

Debian bind DNS Cache Poisoning Vulnerability - Secunia Advisories - Vulnerability Intelligence - Secunia.com

IBM Corporation Information for VU#800113

[SECURITY] Fedora 8 Update: bind-9.5.0-28.P1.fc8

Blue Coat ProxySG DNS Cache Poisoning Vulnerability - Advisories - Secunia

Blue Coat ProxySG DNS Cache Poisoning Vulnerability - Advisories - Secunia
NetBSD-SA2008-009
The Slackware Linux Project: Slackware Security Advisories
Nominum CNS and Vantio DNS Cache Poisoning Vulnerability - Advisories - Secunia
ISC BIND Query Port DNS Cache Poisoning - Secunia Advisories - Vulnerability Intelligence - Secunia.com
CVE Program record
NVD vulnerability detail

Vendor Comments And Credit

Organization	Published	Contributor	Statement
Red Hat	2008-07-09	Mark J Cox	http://rhn.redhat.com/errata/RHSA-2008-0533.html

There are currently no legacy QID mappings associated with this CVE.