CVE-2009-0159

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

Summary

CVE	CVE-2009-0159
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2009-04-14 15:30:00 UTC
Updated	2018-10-11 21:00:00 UTC
Description	Stack-based buffer overflow in the cookedprint function in ntpq/ntpq.c in ntpq in NTP before 4.2.4p7-RC2 allows remote NT

Risk And Classification

Problem Types: CWE-119

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Ntp	Ntp	4.0.72	All	All	All
Application	Ntp	Ntp	4.0.73	All	All	All
Application	Ntp	Ntp	4.0.90	All	All	All
Application	Ntp	Ntp	4.0.91	All	All	All
Application	Ntp	Ntp	4.0.92	All	All	All
Application	Ntp	Ntp	4.0.93	All	All	All
Application	Ntp	Ntp	4.0.94	All	All	All
Application	Ntp	Ntp	4.0.95	All	All	All
Application	Ntp	Ntp	4.0.96	All	All	All
Application	Ntp	Ntp	4.0.97	All	All	All
Application	Ntp	Ntp	4.0.98	All	All	All
Application	Ntp	Ntp	4.0.99	All	All	All
Application	Ntp	Ntp	4.1.0	All	All	All
Application	Ntp	Ntp	4.1.2	All	All	All
Application	Ntp	Ntp	4.2.0	All	All	All
Application	Ntp	Ntp	4.2.2	All	All	All
Application	Ntp	Ntp	4.2.2p1	All	All	All

Application	Ntp	Ntp	4.2.2p2	All	All	All
Application	Ntp	Ntp	4.2.2p3	All	All	All
Application	Ntp	Ntp	4.2.2p4	All	All	All
Application	Ntp	Ntp	4.2.4	All	All	All
Application	Ntp	Ntp	4.2.4p0	All	All	All
Application	Ntp	Ntp	4.2.4p1	All	All	All
Application	Ntp	Ntp	4.2.4p2	All	All	All
Application	Ntp	Ntp	4.2.4p3	All	All	All
Application	Ntp	Ntp	4.2.4p4	All	All	All
Application	Ntp	Ntp	4.2.4p5	All	All	All
Application	Ntp	Ntp	4.2.4p6	All	All	All
Application	Ntp	Ntp	4.0.72	All	All	All
Application	Ntp	Ntp	4.0.73	All	All	All
Application	Ntp	Ntp	4.0.90	All	All	All
Application	Ntp	Ntp	4.0.91	All	All	All
Application	Ntp	Ntp	4.0.92	All	All	All
Application	Ntp	Ntp	4.0.93	All	All	All
Application	Ntp	Ntp	4.0.94	All	All	All
Application	Ntp	Ntp	4.0.95	All	All	All
Application	Ntp	Ntp	4.0.96	All	All	All
Application	Ntp	Ntp	4.0.97	All	All	All
Application	Ntp	Ntp	4.0.98	All	All	All
Application	Ntp	Ntp	4.0.99	All	All	All
Application	Ntp	Ntp	4.1.0	All	All	All
Application	Ntp	Ntp	4.1.2	All	All	All
Application	Ntp	Ntp	4.2.0	All	All	All
Application	Ntp	Ntp	4.2.2	All	All	All
Application	Ntp	Ntp	4.2.2p1	All	All	All
Application	Ntp	Ntp	4.2.2p2	All	All	All
Application	Ntp	Ntp	4.2.2p3	All	All	All
Application	Ntp	Ntp	4.2.2p4	All	All	All
Application	Ntp	Ntp	4.2.4	All	All	All
Application	Ntp	Ntp	4.2.4p0	All	All	All
Application	Ntp	Ntp	4.2.4p1	All	All	All
Application	Ntp	Ntp	4.2.4p2	All	All	All

Application	Ntp	Ntp	4.2.4p3	All	All	All
Application	Ntp	Ntp	4.2.4p4	All	All	All
Application	Ntp	Ntp	4.2.4p5	All	All	All
Application	Ntp	Ntp	4.2.4p6	All	All	All
Application	Ntp	Ntp	All	rc1	All	All

References

Reference	Source
490617 – (CVE-2009-0159) CVE-2009-0159 ntp: buffer overflow in ntpq	CONFIRM
Gentoo Linux Documentation -- NTP: Remote execution of arbitrary code	GENTOO
NTP 'ntpq' Stack Buffer Overflow Vulnerability	BID
ntp Buffer Overflow in ntpq cookedprint() Lets Remote Users Execute Arbitrary Code - SecurityTracker	SECTRACK
NetBSD update for ntp - Secunia Advisories - Vulnerability Information - Secunia.com	SECUNIA
NetBSD-SA2009-006	NETBSD
Support / Security / Advisories / / MDVSA-2009:092 | Mandriva	MANDRIVA
bugs.pardus.org.tr/show_bug.cgi	CONFIRM
Fedora update for ntp - Secunia Advisories - Vulnerability Information - Secunia.com	SECUNIA
USN-777-1: Ntp vulnerabilities | Ubuntu security notices	UBUNTU
Repository / Oval Repository	OVAL
rhn.redhat.com | Red Hat Support	REDHAT
SecurityFocus	BUGTRAQ
ntp.bkbits.net/ntp-stable	CONFIRM
Repository / Oval Repository	OVAL
Debian -- Security Information -- DSA-1801-1 ntp	DEBIAN
[SECURITY] Fedora 9 Update: ntp-4.2.4p7-1.fc9	FEDORA
Apple Mac OS X Security Update Fixes Multiple Vulnerabilities - Secunia Advisories - Vulnerability Information - Secunia.com	SECUNIA
[SECURITY] Fedora 10 Update: ntp-4.2.4p7-1.fc10	FEDORA
Webmail : Solution de messagerie professionnelle - OVHcloud- OVH	VUPEN
About the security content of Security Update 2009-002 / Mac OS X v10.5.7	CONFIRM
US-CERT Technical Cyber Security Alert TA09-133A -- Apple Updates for Multiple Vulnerabilities	CERT
Webmail : Solution de messagerie professionnelle - OVHcloud- OVH	VUPEN
Red Hat update for ntp - Secunia Advisories - Vulnerability Information - Secunia.com	SECUNIA
53593	OSVDB
Repository / Oval Repository	OVAL
'[security bulletin] HPSBUX02859 SSRT101144 rev.1 - HP-UX Running XNTP, Remote Denial of Service (DoS' - MARC	HP
SUSE Update for Multiple Packages - Advisories - Community	SECUNIA

IBM X-Force Exchange	XF
Repository / Oval Repository	OVAL
Webmail : Solution de messagerie professionnelle - OVHcloud- OVH	VUPEN
Gentoo update for ntp - Secunia Advisories - Vulnerability Information - Secunia.com	SECUNIA
Debian update for ntp - Secunia Advisories - Vulnerability Information - Secunia.com	SECUNIA
Bug 1144 – limited buffer overflow in ntpq. CVE-2009-0159	CONFIRM
rhn.redhat.com | Red Hat Support	REDHAT
rhn.redhat.com | Red Hat Support	REDHAT
The Slackware Linux Project: Slackware Security Advisories	SLACKWARE
Repository / Oval Repository	OVAL
Red hat update for ntp - Secunia Advisories - Vulnerability Information - Secunia.com	SECUNIA
APPLE-SA-2009-05-12 Security Update 2009-002 / Mac OS X v10.5.7	APPLE
VMSA-2009-0016.1	CONFIRM
Slackware update for ntp - Secunia.com	SECUNIA
NTP ntpq "cookedprint()" Buffer Overflow Vulnerability - Secunia Advisories - Vulnerability Information - Secunia.com	SECUNIA
Ubuntu update for ntp - Secunia.com	SECUNIA
[security-announce] SUSE Security Summary Report: SUSE-SR:2009:011	SUSE
VMware ESX and vMA Update for Multiple Packages - Secunia Advisories - Vulnerability Information - Secunia.com	SECUNIA
CVE Program record	CVE.ORG
NVD vulnerability detail	NVD

No vendor comments have been submitted for this CVE.

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