# CVE-2009-3563

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

## Summary

| | |
|---|---|
| **CVE** | CVE-2009-3563 |
| **State** | PUBLISHED |
| **Assigner** | mitre |
| **Source Priority** | CVE Program / NVD first with legacy fallback |
| **Published** | 2009-12-09 18:30:00 UTC |
| **Updated** | 2026-04-23 00:35:47 UTC |
| **Description** | ntp_request.c in ntpd in NTP before 4.2.4p8, and 4.2.5, allows remote attackers to cause a denial of service (CPU and banc |

## Risk And Classification

**Primary CVSS:** v2.0 6.4 from nvd@nist.gov

AV:N/AC:L/Au:N/C:N/I:P/A:P

**Problem Types:** NVD-CWE-Other | n/a

## CVSS v2.0 Breakdown

Access Vector

Network

Access Complexity

Low

Authentication

None

Confidentiality

None

Integrity

Partial

Availability

Partial

AV:N/AC:L/Au:N/C:N/I:P/A:P

## 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 | 4.2.5 | All | All | All |
| Application | Ntp | Ntp | All | All | All | All |

## Vendor Declared Affected Products

| Source | Vendor | Product | Version | Platforms |
|---|---|---|---|---|
| CNA | Na | N/a | affected n/a | Not specified |

## References

| Reference | Source |
|---|---|
| VMware ESX Server Multiple Vulnerabilities - Advisories - Community | af854a3a-2127-42 |
| sunsolve.sun.com/search/document.do | af854a3a-2127-42 |
| aix.software.ibm.com/aix/efixes/security/xntpd_advisory.asc | af854a3a-2127-42 |
| VMware vMA Update for Multiple Packages - Advisories - Community | af854a3a-2127-42 |
| ftp.netbsd.org/pub/NetBSD/security/advisories/NetBSD-SA2010-005.txt.asc | af854a3a-2127-42 |
| ASA-2009-591 (RHSA-2009-1648) | af854a3a-2127-42 |
| Webmail : Solution de messagerie professionnelle - OVHcloud- OVH | af854a3a-2127-42 |
| NTP Mode 7 Request Denial of Service - Secunia Advisories - Vulnerability Information - Secunia.com | af854a3a-2127-42 |
| Webmail : Solution de messagerie professionnelle - OVHcloud- OVH | af854a3a-2127-42 |
| Juniper Networks - 2015-04 Security Bulletin: IDP: Multiple vulnerabilities addressed by third party software updates | af854a3a-2127-42 |

| | |
|---|---|
| Juniper Networks - 2015-04 Security Bulletin: IDP: Multiple vulnerabilities addressed by third party software updates. | af854a3a-2127-42 |
| NTP mode 7 MODE_PRIVATE Packet Remote Denial of Service Vulnerability | af854a3a-2127-42 |
| Debian -- Security Information -- DSA-1948-1 ntp | af854a3a-2127-42 |
| '[security bulletin] HPSBUX02859 SSRT101144 rev.1 - HP-UX Running XNTP, Remote Denial of Service (DoS' - MARC | af854a3a-2127-42 |
| Webmail : Solution de messagerie professionnelle - OVHcloud- OVH | af854a3a-2127-42 |
| US-CERT Vulnerability Note VU#568372 | af854a3a-2127-42 |
| Cisco Systems, Inc. Information for VU#568372 | af854a3a-2127-42 |
| IBM IZ68659: NTP MODE 7 VULNERABILITY IN AIX 5.3 /AIX 6.1 APPLIES TO AIX 5300-08 - United States | af854a3a-2127-42 |
| Bug 1331 – DoS with mode 7 packets (CVE-2009-3563) | af854a3a-2127-42 |
| CVE-2009-3563 | af854a3a-2127-42 |
| '[security bulletin] HPSBUX02639 SSRT100293 rev.1 - HP-UX Running XNTP, Remote Denial of Service (DoS' - MARC | af854a3a-2127-42 |
| 531213 – (CVE-2009-3563) CVE-2009-3563 ntpd: DoS with mode 7 packets (VU#568372) | af854a3a-2127-42 |
| Repository / Oval Repository | af854a3a-2127-42 |
| www.kb.cert.org/vuls/id/417980 | af854a3a-2127-42 |
| Repository / Oval Repository | af854a3a-2127-42 |
| Avaya Products Two Vulnerabilities - Secunia Advisories - Vulnerability Information - Secunia.com | af854a3a-2127-42 |
| [Security-announce] VMSA-2010-0004 ESX Service Console and vMA third party updates | af854a3a-2127-42 |
| [SECURITY] Fedora 10 Update: ntp-4.2.4p7-2.fc10 | af854a3a-2127-42 |
| rhn.redhat.com \| Red Hat Support | af854a3a-2127-42 |
| IBM AIX NTP Mode 7 Request Denial of Service - Secunia.com | af854a3a-2127-42 |
| IBM notice: The page you requested cannot be displayed | af854a3a-2127-42 |
| Red Hat Customer Portal | af854a3a-2127-42 |
| VMware ESX Server 4 Multiple Vulnerabilities - Advisories - Community | af854a3a-2127-42 |
| Repository / Oval Repository | af854a3a-2127-42 |
| NetBSD update for ntp - Advisories - Community | af854a3a-2127-42 |
| [SECURITY] Fedora 11 Update: ntp-4.2.4p7-3.fc11 | af854a3a-2127-42 |
| SecurityTracker.com Archives - NTP Mode 7 Packet Processing Flaw Lets Remote Users Deny Service | af854a3a-2127-42 |
| [ntp:announce] NTP 4.2.4p8 Released | af854a3a-2127-42 |
| Repository / Oval Repository | af854a3a-2127-42 |
| access.redhat.com | af854a3a-2127-42 |
| #560074 - ntp: CVE-2009-3563 DoS through mode 7 packets - Debian Bug report logs | af854a3a-2127-42 |
| SecurityNotice < Main < NTP | af854a3a-2127-42 |
| 2015-07 Security Bulletin: CTPView: Multiple vulnerabilities in CTPView - Juniper Networks | af854a3a-2127-42 |
| QNX Software Systems Inc. Information for VU#568372 | af854a3a-2127-42 |
| 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.

© CVE.report 2026 |
Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, completeness or usefulness of any information, opinion, advice or other content. EACH USER WILL BE SOLELY RESPONSIBLE FOR ANY consequences of his or her direct or indirect use of this web site. ALL WARRANTIES OF ANY KIND ARE EXPRESSLY DISCLAIMED. This site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE, CWE, and OVAL are registred trademarks of The MITRE Corporation and the authoritative source of CVE content is MITRE's CVE web site. This site includes MITRE data granted under the following license.

**Free CVE JSON API** cve.report/api

**CVE.report and Source URL Uptime Status** **status.cve.report**