



CVE-2015-7977

[MITRE](#)[NVD](#)[CVE.ORG](#)[Print: PDF](#)

Summary

CVE	CVE-2015-7977
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2017-01-30 21:59:00 UTC
Updated	2022-02-01 18:13:00 UTC
Description	ntpd in NTP before 4.2.8p6 and 4.3.x before 4.3.90 allows remote attackers to cause a denial of service (NULL pointer dereference) via crafted NTP requests.

Risk And Classification

Problem Types: CWE-476

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Canonical	Ubuntu Linux	12.04	All	All	All
Operating System	Canonical	Ubuntu Linux	14.04	All	All	All
Operating System	Canonical	Ubuntu Linux	16.04	All	All	All
Operating System	Debian	Debian Linux	8.0	All	All	All
Operating System	Debian	Debian Linux	9.0	All	All	All
Operating System	Fedoraproject	Fedora	22	All	All	All
Operating System	Fedoraproject	Fedora	23	All	All	All
Operating System	Freebsd	Freebsd	10.1	-	All	All
Operating System	Freebsd	Freebsd	10.1	p1	All	All
Operating System	Freebsd	Freebsd	10.1	p10	All	All
Operating System	Freebsd	Freebsd	10.1	p12	All	All
Operating System	Freebsd	Freebsd	10.1	p15	All	All
Operating System	Freebsd	Freebsd	10.1	p16	All	All
Operating System	Freebsd	Freebsd	10.1	p17	All	All
Operating System	Freebsd	Freebsd	10.1	p18	All	All
Operating System	Freebsd	Freebsd	10.1	p19	All	All
Operating System	Freebsd	Freebsd	10.1	p2	All	All

Operating System	Freebsd	Freebsd	10.1	p22	All	All
Operating System	Freebsd	Freebsd	10.1	p24	All	All
Operating System	Freebsd	Freebsd	10.1	p25	All	All
Operating System	Freebsd	Freebsd	10.1	p26	All	All
Operating System	Freebsd	Freebsd	10.1	p27	All	All
Operating System	Freebsd	Freebsd	10.1	p3	All	All
Operating System	Freebsd	Freebsd	10.1	p4	All	All
Operating System	Freebsd	Freebsd	10.1	p5	All	All
Operating System	Freebsd	Freebsd	10.1	p6	All	All
Operating System	Freebsd	Freebsd	10.1	p7	All	All
Operating System	Freebsd	Freebsd	10.1	p8	All	All
Operating System	Freebsd	Freebsd	10.1	p9	All	All
Operating System	Freebsd	Freebsd	10.2	-	All	All
Operating System	Freebsd	Freebsd	10.2	p1	All	All
Operating System	Freebsd	Freebsd	10.2	p10	All	All
Operating System	Freebsd	Freebsd	10.2	p2	All	All
Operating System	Freebsd	Freebsd	10.2	p5	All	All
Operating System	Freebsd	Freebsd	10.2	p7	All	All
Operating System	Freebsd	Freebsd	10.2	p8	All	All
Operating System	Freebsd	Freebsd	10.2	p9	All	All
Operating System	Freebsd	Freebsd	9.3	-	All	All
Operating System	Freebsd	Freebsd	9.3	p1	All	All
Operating System	Freebsd	Freebsd	9.3	p10	All	All
Operating System	Freebsd	Freebsd	9.3	p12	All	All
Operating System	Freebsd	Freebsd	9.3	p13	All	All
Operating System	Freebsd	Freebsd	9.3	p16	All	All
Operating System	Freebsd	Freebsd	9.3	p19	All	All
Operating System	Freebsd	Freebsd	9.3	p2	All	All
Operating System	Freebsd	Freebsd	9.3	p20	All	All
Operating System	Freebsd	Freebsd	9.3	p21	All	All
Operating System	Freebsd	Freebsd	9.3	p22	All	All
Operating System	Freebsd	Freebsd	9.3	p23	All	All
Operating System	Freebsd	Freebsd	9.3	p24	All	All
Operating System	Freebsd	Freebsd	9.3	p25	All	All
Operating System	Freebsd	Freebsd	9.3	p28	All	All

Operating System	Freebsd	Freebsd	9.3	p3	All	All
Operating System	Freebsd	Freebsd	9.3	p30	All	All
Operating System	Freebsd	Freebsd	9.3	p31	All	All
Operating System	Freebsd	Freebsd	9.3	p32	All	All
Operating System	Freebsd	Freebsd	9.3	p33	All	All
Operating System	Freebsd	Freebsd	9.3	p34	All	All
Operating System	Freebsd	Freebsd	9.3	p5	All	All
Operating System	Freebsd	Freebsd	9.3	p6	All	All
Operating System	Freebsd	Freebsd	9.3	p7	All	All
Operating System	Freebsd	Freebsd	9.3	p8	All	All
Operating System	Freebsd	Freebsd	9.3	p9	All	All
Application	Netapp	Clustered Data Ontap	-	All	All	All
Application	Netapp	Oncommand Balance	-	All	All	All
Application	Ntp	Ntp	All	All	All	All
Application	Ntp	Ntp	4.2.8	-	All	All
Application	Ntp	Ntp	4.2.8	p1	All	All
Application	Ntp	Ntp	4.2.8	p1-beta1	All	All
Application	Ntp	Ntp	4.2.8	p1-beta2	All	All
Application	Ntp	Ntp	4.2.8	p1-beta3	All	All
Application	Ntp	Ntp	4.2.8	p1-beta4	All	All
Application	Ntp	Ntp	4.2.8	p1-beta5	All	All
Application	Ntp	Ntp	4.2.8	p1-rc1	All	All
Application	Ntp	Ntp	4.2.8	p1-rc2	All	All
Application	Ntp	Ntp	4.2.8	p2	All	All
Application	Ntp	Ntp	4.2.8	p2-rc1	All	All
Application	Ntp	Ntp	4.2.8	p2-rc2	All	All
Application	Ntp	Ntp	4.2.8	p2-rc3	All	All
Application	Ntp	Ntp	4.2.8	p3	All	All
Application	Ntp	Ntp	4.2.8	p3-rc1	All	All
Application	Ntp	Ntp	4.2.8	p3-rc2	All	All
Application	Ntp	Ntp	4.2.8	p3-rc3	All	All
Application	Ntp	Ntp	4.2.8	p4	All	All
Application	Ntp	Ntp	4.2.8	p5	All	All
Application	Ntp	Ntp	4.3.0	All	All	All
Application	Ntp	Ntp	4.3.1	All	All	All

Application	Ntp	Ntp	4.3.10	All	All	All
Application	Ntp	Ntp	4.3.11	All	All	All
Application	Ntp	Ntp	4.3.12	All	All	All
Application	Ntp	Ntp	4.3.13	All	All	All
Application	Ntp	Ntp	4.3.14	All	All	All
Application	Ntp	Ntp	4.3.15	All	All	All
Application	Ntp	Ntp	4.3.16	All	All	All
Application	Ntp	Ntp	4.3.17	All	All	All
Application	Ntp	Ntp	4.3.18	All	All	All
Application	Ntp	Ntp	4.3.19	All	All	All
Application	Ntp	Ntp	4.3.2	All	All	All
Application	Ntp	Ntp	4.3.20	All	All	All
Application	Ntp	Ntp	4.3.21	All	All	All
Application	Ntp	Ntp	4.3.22	All	All	All
Application	Ntp	Ntp	4.3.23	All	All	All
Application	Ntp	Ntp	4.3.24	All	All	All
Application	Ntp	Ntp	4.3.25	All	All	All
Application	Ntp	Ntp	4.3.26	All	All	All
Application	Ntp	Ntp	4.3.27	All	All	All
Application	Ntp	Ntp	4.3.28	All	All	All
Application	Ntp	Ntp	4.3.29	All	All	All
Application	Ntp	Ntp	4.3.3	All	All	All
Application	Ntp	Ntp	4.3.30	All	All	All
Application	Ntp	Ntp	4.3.31	All	All	All
Application	Ntp	Ntp	4.3.32	All	All	All
Application	Ntp	Ntp	4.3.33	All	All	All
Application	Ntp	Ntp	4.3.34	All	All	All
Application	Ntp	Ntp	4.3.35	All	All	All
Application	Ntp	Ntp	4.3.36	All	All	All
Application	Ntp	Ntp	4.3.37	All	All	All
Application	Ntp	Ntp	4.3.38	All	All	All
Application	Ntp	Ntp	4.3.39	All	All	All
Application	Ntp	Ntp	4.3.4	All	All	All
Application	Ntp	Ntp	4.3.40	All	All	All
Application	Ntp	Ntp	4.3.41	All	All	All
Application	Ntp	Ntp	4.3.42	All	All	All

Application	Ntp	Ntp	4.3.43	All	All	All
Application	Ntp	Ntp	4.3.44	All	All	All
Application	Ntp	Ntp	4.3.45	All	All	All
Application	Ntp	Ntp	4.3.46	All	All	All
Application	Ntp	Ntp	4.3.47	All	All	All
Application	Ntp	Ntp	4.3.48	All	All	All
Application	Ntp	Ntp	4.3.49	All	All	All
Application	Ntp	Ntp	4.3.5	All	All	All
Application	Ntp	Ntp	4.3.50	All	All	All
Application	Ntp	Ntp	4.3.51	All	All	All
Application	Ntp	Ntp	4.3.52	All	All	All
Application	Ntp	Ntp	4.3.53	All	All	All
Application	Ntp	Ntp	4.3.54	All	All	All
Application	Ntp	Ntp	4.3.55	All	All	All
Application	Ntp	Ntp	4.3.56	All	All	All
Application	Ntp	Ntp	4.3.57	All	All	All
Application	Ntp	Ntp	4.3.58	All	All	All
Application	Ntp	Ntp	4.3.59	All	All	All
Application	Ntp	Ntp	4.3.6	All	All	All
Application	Ntp	Ntp	4.3.60	All	All	All
Application	Ntp	Ntp	4.3.61	All	All	All
Application	Ntp	Ntp	4.3.62	All	All	All
Application	Ntp	Ntp	4.3.63	All	All	All
Application	Ntp	Ntp	4.3.64	All	All	All
Application	Ntp	Ntp	4.3.65	All	All	All
Application	Ntp	Ntp	4.3.66	All	All	All
Application	Ntp	Ntp	4.3.67	All	All	All
Application	Ntp	Ntp	4.3.68	All	All	All
Application	Ntp	Ntp	4.3.69	All	All	All
Application	Ntp	Ntp	4.3.7	All	All	All
Application	Ntp	Ntp	4.3.70	All	All	All
Application	Ntp	Ntp	4.3.71	All	All	All
Application	Ntp	Ntp	4.3.72	All	All	All
Application	Ntp	Ntp	4.3.73	All	All	All
Application	Ntp	Ntp	4.3.74	All	All	All

Application	Ntp	Ntp	4.3.75	All	All	All
Application	Ntp	Ntp	4.3.76	All	All	All
Application	Ntp	Ntp	4.3.77	All	All	All
Application	Ntp	Ntp	4.3.78	All	All	All
Application	Ntp	Ntp	4.3.79	All	All	All
Application	Ntp	Ntp	4.3.8	All	All	All
Application	Ntp	Ntp	4.3.80	All	All	All
Application	Ntp	Ntp	4.3.81	All	All	All
Application	Ntp	Ntp	4.3.82	All	All	All
Application	Ntp	Ntp	4.3.83	All	All	All
Application	Ntp	Ntp	4.3.84	All	All	All
Application	Ntp	Ntp	4.3.85	All	All	All
Application	Ntp	Ntp	4.3.86	All	All	All
Application	Ntp	Ntp	4.3.87	All	All	All
Application	Ntp	Ntp	4.3.88	All	All	All
Application	Ntp	Ntp	4.3.89	All	All	All
Application	Ntp	Ntp	4.3.0	All	All	All
Application	Ntp	Ntp	4.3.1	All	All	All
Application	Ntp	Ntp	4.3.10	All	All	All
Application	Ntp	Ntp	4.3.11	All	All	All
Application	Ntp	Ntp	4.3.12	All	All	All
Application	Ntp	Ntp	4.3.13	All	All	All
Application	Ntp	Ntp	4.3.14	All	All	All
Application	Ntp	Ntp	4.3.15	All	All	All
Application	Ntp	Ntp	4.3.16	All	All	All
Application	Ntp	Ntp	4.3.17	All	All	All
Application	Ntp	Ntp	4.3.18	All	All	All
Application	Ntp	Ntp	4.3.19	All	All	All
Application	Ntp	Ntp	4.3.2	All	All	All
Application	Ntp	Ntp	4.3.20	All	All	All
Application	Ntp	Ntp	4.3.21	All	All	All
Application	Ntp	Ntp	4.3.22	All	All	All
Application	Ntp	Ntp	4.3.23	All	All	All
Application	Ntp	Ntp	4.3.24	All	All	All
Application	Ntp	Ntp	4.3.25	All	All	All
Application	Ntp	Ntp	4.3.26	All	All	All


Application	Ntp	Ntp	4.3.26	All	All	All
Application	Ntp	Ntp	4.3.27	All	All	All
Application	Ntp	Ntp	4.3.28	All	All	All
Application	Ntp	Ntp	4.3.29	All	All	All
Application	Ntp	Ntp	4.3.3	All	All	All
Application	Ntp	Ntp	4.3.30	All	All	All
Application	Ntp	Ntp	4.3.31	All	All	All
Application	Ntp	Ntp	4.3.32	All	All	All
Application	Ntp	Ntp	4.3.33	All	All	All
Application	Ntp	Ntp	4.3.34	All	All	All
Application	Ntp	Ntp	4.3.35	All	All	All
Application	Ntp	Ntp	4.3.36	All	All	All
Application	Ntp	Ntp	4.3.37	All	All	All
Application	Ntp	Ntp	4.3.38	All	All	All
Application	Ntp	Ntp	4.3.39	All	All	All
Application	Ntp	Ntp	4.3.4	All	All	All
Application	Ntp	Ntp	4.3.40	All	All	All
Application	Ntp	Ntp	4.3.41	All	All	All
Application	Ntp	Ntp	4.3.42	All	All	All
Application	Ntp	Ntp	4.3.43	All	All	All
Application	Ntp	Ntp	4.3.44	All	All	All
Application	Ntp	Ntp	4.3.45	All	All	All
Application	Ntp	Ntp	4.3.46	All	All	All
Application	Ntp	Ntp	4.3.47	All	All	All
Application	Ntp	Ntp	4.3.48	All	All	All
Application	Ntp	Ntp	4.3.49	All	All	All
Application	Ntp	Ntp	4.3.5	All	All	All
Application	Ntp	Ntp	4.3.50	All	All	All
Application	Ntp	Ntp	4.3.51	All	All	All
Application	Ntp	Ntp	4.3.52	All	All	All
Application	Ntp	Ntp	4.3.53	All	All	All
Application	Ntp	Ntp	4.3.54	All	All	All
Application	Ntp	Ntp	4.3.55	All	All	All
Application	Ntp	Ntp	4.3.56	All	All	All
Application	Ntp	Ntp	4.3.57	All	All	All
Application	Ntp	Ntp	4.3.58	All	All	All

Application	Ntp	Ntp	4.3.59	All	All	All
Application	Ntp	Ntp	4.3.6	All	All	All
Application	Ntp	Ntp	4.3.60	All	All	All
Application	Ntp	Ntp	4.3.61	All	All	All
Application	Ntp	Ntp	4.3.62	All	All	All
Application	Ntp	Ntp	4.3.63	All	All	All
Application	Ntp	Ntp	4.3.64	All	All	All
Application	Ntp	Ntp	4.3.65	All	All	All
Application	Ntp	Ntp	4.3.66	All	All	All
Application	Ntp	Ntp	4.3.67	All	All	All
Application	Ntp	Ntp	4.3.68	All	All	All
Application	Ntp	Ntp	4.3.69	All	All	All
Application	Ntp	Ntp	4.3.7	All	All	All
Application	Ntp	Ntp	4.3.70	All	All	All
Application	Ntp	Ntp	4.3.71	All	All	All
Application	Ntp	Ntp	4.3.72	All	All	All
Application	Ntp	Ntp	4.3.73	All	All	All
Application	Ntp	Ntp	4.3.74	All	All	All
Application	Ntp	Ntp	4.3.75	All	All	All
Application	Ntp	Ntp	4.3.76	All	All	All
Application	Ntp	Ntp	4.3.77	All	All	All
Application	Ntp	Ntp	4.3.78	All	All	All
Application	Ntp	Ntp	4.3.79	All	All	All
Application	Ntp	Ntp	4.3.8	All	All	All
Application	Ntp	Ntp	4.3.80	All	All	All
Application	Ntp	Ntp	4.3.81	All	All	All
Application	Ntp	Ntp	4.3.82	All	All	All
Application	Ntp	Ntp	4.3.83	All	All	All
Application	Ntp	Ntp	4.3.84	All	All	All
Application	Ntp	Ntp	4.3.85	All	All	All
Application	Ntp	Ntp	4.3.86	All	All	All
Application	Ntp	Ntp	4.3.87	All	All	All
Application	Ntp	Ntp	4.3.88	All	All	All
Application	Ntp	Ntp	4.3.89	All	All	All
Application	Ntp	Ntp	All	All	All	All

Application	Ntp	Ntp	All	p5	All	All
Operating System	Oracle	Linux	6	-	All	All
Hardware	Siemens	Tim 4r-ie	All	All	All	All
Hardware	Siemens	Tim 4r-ie Dnp3	-	All	All	All
Operating System	Siemens	Tim 4r-ie Dnp3 Firmware	-	All	All	All
Operating System	Siemens	Tim 4r-ie Firmware	All	All	All	All
Hardware	Siemnes	Tim 4r-ie	All	All	All	All
Hardware	Siemnes	Tim 4r-ie Dnp3	-	All	All	All
Operating System	Siemnes	Tim 4r-ie Dnp3 Firmware	-	All	All	All
Operating System	Siemnes	Tim 4r-ie Firmware	All	All	All	All

References

Reference	Source
support.ntp.org/bin/view/Main/SecurityNotice	CONF
[security-announce] SUSE-SU-2016:1247-1: important: Security update for	SUSE
NTP: Multiple vulnerabilities (GLSA 201607-15) — Gentoo Security	GENT
openSUSE-SU-2016:1423-1: moderate: Security update for ntp	SUSE
[SECURITY] Fedora 23 Update: ntp-4.2.6p5-36.fc23	FEDO
Oracle Linux Bulletin - April 2016	CONF
[security-announce] SUSE-SU-2016:1311-1: important: Security update for	SUSE
Vulnerability Note VU#718152 - NTP.org ntpd contains multiple vulnerabilities	CERT
support.ntp.org/bin/view/Main/NtpBug2939	CONF
ntp Multiple Flaws Let Remote Users Spoof Messages, Obtain Potentially Sensitive Information, and Deny Service - SecurityTracker	SECTI
[security-announce] SUSE-SU-2016:1912-1: important: Security update for	SUSE
January 2016 Network Time Protocol Daemon (ntpd) Vulnerabilities in NetApp Products NetApp Product Security	CONF
Red Hat Customer Portal	REDH
[security-announce] SUSE-SU-2016:2094-1: important: Security update for	SUSE
SA113: January 2016 NTP Security Vulnerabilities Blue Coat Systems, Inc.	CONF
FreeBSD-SA-16:09	FREEI
[security-announce] SUSE-SU-2016:1177-1: important: Security update for	SUSE
Siemens TIM 4R-IE Devices CISA	CONF
NTP CVE-2015-7977 NULL Pointer Dereference Denial of Service Vulnerability	BID
[security-announce] openSUSE-SU-2016:1292-1: important: Security update	SUSE
[SECURITY] Fedora 22 Update: ntp-4.2.6p5-36.fc22	FEDO
cert-portal.siemens.com/productcert/pdf/ssa-497656.pdf	CONF
Red Hat Customer Portal	REDH

Multiple Vulnerabilities in Network Time Protocol Daemon Affecting Cisco Products - January 2016	CISCC
[security-announce] SUSE-SU-2016:1175-1: important: Security update for	SUSE
USN-3096-1: NTP vulnerabilities Ubuntu	UBUN
Debian -- Security Information -- DSA-3629-1 ntp	DEBIA
CVE Program record	CVE.C
NVD vulnerability detail	NVD
	
<p>No vendor comments have been submitted for this CVE.</p>	
<p>Legacy QID Mappings</p>	
<p>590721 Siemens TIM 4R-IE Devices Multiple Vulnerabilities (ICSA-21-103-11)</p>	

© [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 registered 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](#).

CVE.report and Source URL Uptime Status [status.cve.report](#)