



CVE-2020-15025

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

Summary

CVE	CVE-2020-15025
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2020-06-24 19:15:00 UTC
Updated	2023-11-07 03:17:00 UTC
Description	ntpd in ntp 4.2.8 before 4.2.8p15 and 4.3.x before 4.3.101 allows remote attackers to cause a denial of service (memory co

Risk And Classification

Problem Types: CWE-401

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Hardware	Netapp	8300	-	All	All	All
Operating System	Netapp	8300 Firmware	-	All	All	All
Hardware	Netapp	8700	-	All	All	All
Operating System	Netapp	8700 Firmware	-	All	All	All
Hardware	Netapp	A400	-	All	All	All
Operating System	Netapp	A400 Firmware	-	All	All	All
Application	Netapp	Cloud Backup	-	All	All	All
Hardware	Netapp	H300e	-	All	All	All
Operating System	Netapp	H300e Firmware	-	All	All	All
Hardware	Netapp	H300s	-	All	All	All
Operating System	Netapp	H300s Firmware	-	All	All	All
Hardware	Netapp	H410c	-	All	All	All
Operating System	Netapp	H410c Firmware	-	All	All	All
Hardware	Netapp	H410s	-	All	All	All
Operating System	Netapp	H410s Firmware	-	All	All	All
Hardware	Netapp	H500e	-	All	All	All
Operating System	Netapp	H500e Firmware	-	All	All	All

Hardware	Netapp	H500s	-	All	All	All
Operating System	Netapp	H500s Firmware	-	All	All	All
Hardware	Netapp	H700e	-	All	All	All
Operating System	Netapp	H700e Firmware	-	All	All	All
Hardware	Netapp	H700s	-	All	All	All
Operating System	Netapp	H700s Firmware	-	All	All	All
Application	Netapp	Steelstore Cloud Integrated Storage	-	All	All	All
Application	Ntp	Ntp	All	All	All	All
Application	Ntp	Ntp	4.2.8	p11	All	All
Application	Ntp	Ntp	4.2.8	p12	All	All
Application	Ntp	Ntp	4.2.8	p13	All	All
Application	Ntp	Ntp	4.2.8	p14	All	All
Application	Ntp	Ntp	All	All	All	All
Application	Ntp	Ntp	4.2.8	p11	All	All
Application	Ntp	Ntp	4.2.8	p12	All	All
Application	Ntp	Ntp	4.2.8	p13	All	All
Application	Ntp	Ntp	4.2.8	p14	All	All
Operating System	Opensuse	Leap	15.1	All	All	All
Operating System	Opensuse	Leap	15.2	All	All	All
Application	Oracle	Zfs Storage Appliance Kit	8.8	All	All	All

References

Reference	Source	Link
NTP: Multiple vulnerabilities (GLSA 202007-12) — Gentoo security	GENTOO	security.gentoo.org
support.ntp.org/bin/view/Main/NtpBug3661	MISC	support.ntp.org
SecurityNotice < Main < NTP	MISC	support.ntp.org
CVE-2020-15025 Network Time Protocol Daemon (ntpd) Vulnerability in NetApp Products NetApp Product Security	CONFIRM	security.netapp.com
[security-announce] openSUSE-SU-2020:0934-1: moderate: Security update for ntp	SUSE	lists.opensuse.org
729458 – (CVE-2020-15025) <net-misc/ntp-4.2.8_p15: Memory leak allowing denial of service (CVE-2020-15025)	MISC	bugs.gentoo.org
[security-announce] openSUSE-SU-2020:1007-1: moderate: Security update for ntp	SUSE	lists.opensuse.org
Oracle Critical Patch Update Advisory - January 2021	MISC	www.oracle.com
CVE Program record	CVE.ORG	www.cve.org
NVD vulnerability detail	NVD	nvd.nist.gov

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

[296071](#) Oracle Solaris 11.4 Support Repository Update (SRU) 27.82.1 Missing (CPUOCT2020)

[38891](#) Network Time Protocol Denial of Service (DoS) Vulnerability (ntp-4.2.8p15,ntp-4.3.101)

© [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](#)