



# CVE-2015-7974

[MITRE](#)[NVD](#)[CVE.ORG](#)[Print: PDF !\[\]\(e3f8612927870f2e0f9f5989e6dd3064\_img.jpg\)](#)

## Summary

<b>CVE</b>	CVE-2015-7974
<b>State</b>	PUBLIC
<b>Assigner</b>	cve@mitre.org
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2016-01-26 19:59:00 UTC
<b>Updated</b>	2021-04-26 17:42:00 UTC
<b>Description</b>	NTP 4.x before 4.2.8p6 and 4.3.x before 4.3.90 do not verify peer associations of symmetric keys when authenticating pack

## Risk And Classification

**Problem Types:** CWE-287

## NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Debian	Debian Linux	8.0	All	All	All
Operating System	Debian	Debian Linux	9.0	All	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	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
Hardware	Siemens	Tim 4r-ie	-	All	All	All
Hardware	Siemens	Tim 4r-ie Dnp3	-	All	All	All
Operating System	Siemens	Tim 4r-ie Dnp3 Firmware	All	All	All	All
Operating System	Siemens	Tim 4r-ie Firmware	All	All	All	All

## References

Reference	Source
NTP CVE-2015-7974 Symmetric Key Encryption Authentication Security Bypass Vulnerability	BID

Document Display   HPE Support Center	CONF
NTP: Multiple vulnerabilities (GLSA 201607-15) — Gentoo Security	GENT
Siemens TIM 4R-IE Devices   CISA	MISC
Cisco Talos - Talos 2016 0071	MISC
ntp Multiple Flaws Let Remote Users Spoof Messages, Obtain Potentially Sensitive Information, and Deny Service - SecurityTracker	SECTI
January 2016 Network Time Protocol Daemon (ntpd) Vulnerabilities in NetApp Products   NetApp Product Security	CONF
FreeBSD-SA-16:09	FREED
Document Display   HPE Support Center	CONF
support.ntp.org/bin/view/Main/NtpBug2936	CONF
Bug 2936 – Skeleton Key: Any system knowing the trusted key can serve time	CONF
cert-portal.siemens.com/productcert/pdf/ssa-497656.pdf	CONF
Red Hat Customer Portal	REDH
Debian -- Security Information -- DSA-3629-1 ntp	DEBIAN
CVE Program record	CVE.C
NVD vulnerability detail	NVD

No vendor comments have been submitted for this CVE.

#### Legacy QID Mappings

[590721](#) Siemens TIM 4R-IE Devices Multiple Vulnerabilities (ICSA-21-103-11)

© [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](#)