



# CVE-2014-9751

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

## Summary

|                        |  |
|------------------------|--|
| <b>CVE</b>             | CVE-2014-9751  |
| <b>State</b>           | PUBLIC   |
| <b>Assigner</b>        | cve@mitre.org  |
| <b>Source Priority</b> | CVE Program / NVD first with legacy fallback   |
| <b>Published</b>       | 2015-10-06 01:59:00 UTC  |
| <b>Updated</b>         | 2021-09-08 17:19:00 UTC  |
| <b>Description</b>     | The read_network_packet function in ntp_io.c in ntpd in NTP 4.x before 4.2.8p1 on Linux and OS X does not properly deter |

## Risk And Classification

### Problem Types: CWE-20

## NVD Known Affected Configurations (CPE 2.3)

| Type             | Vendor                 | Product                      | Version | Update | Edition | Language |
|------------------|------------------------|------------------------------|---------|--------|---------|----------|
| Operating System | <a href="#">Apple</a>  | <a href="#">Macos</a>        | -       | All    | All     | All      |
| Operating System | <a href="#">Apple</a>  | <a href="#">Mac Os</a>       | -       | All    | All     | All      |
| Operating System | <a href="#">Apple</a>  | <a href="#">Mac Os</a>       | -       | All    | All     | All      |
| Operating System | <a href="#">Debian</a> | <a href="#">Debian Linux</a> | 7.0     | All    | All     | All      |
| Operating System | <a href="#">Debian</a> | <a href="#">Debian Linux</a> | 8.0     | All    | All     | All      |
| Operating System | <a href="#">Debian</a> | <a href="#">Debian Linux</a> | 9.0     | All    | All     | All      |
| Operating System | <a href="#">Debian</a> | <a href="#">Debian Linux</a> | 7.0     | All    | All     | All      |
| Operating System | <a href="#">Debian</a> | <a href="#">Debian Linux</a> | 8.0     | All    | All     | All      |
| Operating System | <a href="#">Debian</a> | <a href="#">Debian Linux</a> | 9.0     | All    | All     | All      |
| Operating System | <a href="#">Linux</a>  | <a href="#">Linux Kernel</a> | -       | All    | All     | All      |
| Operating System | <a href="#">Linux</a>  | <a href="#">Linux Kernel</a> | -       | All    | All     | All      |
| Application      | <a href="#">Ntp</a>    | <a href="#">Ntp</a>          | All     | All    | All     | All      |
| Application      | <a href="#">Ntp</a>    | <a href="#">Ntp</a>          | 4.2.8   | -      | All     | All      |
| Application      | <a href="#">Ntp</a>    | <a href="#">Ntp</a>          | All     | All    | All     | All      |
| Application      | <a href="#">Ntp</a>    | <a href="#">Ntp</a>          | 4.2.8   | -      | All     | All      |
| Operating System | <a href="#">Oracle</a> | <a href="#">Linux</a>        | 7       | -      | All     | All      |
| Operating System | <a href="#">Oracle</a> | <a href="#">Linux</a>        | 7       | -      | All     | All      |

|                  |                        |  |     |     |     |     |
|------------------|------------------------|--|-----|-----|-----|-----|
| Operating System | <a href="#">Redhat</a> | <a href="#">Enterprise Linux Desktop</a>     | 6.0 | All | All | All |
| Operating System | <a href="#">Redhat</a> | <a href="#">Enterprise Linux Desktop</a>     | 6.0 | All | All | All |
| Operating System | <a href="#">Redhat</a> | <a href="#">Enterprise Linux Server</a>      | 6.0 | All | All | All |
| Operating System | <a href="#">Redhat</a> | <a href="#">Enterprise Linux Server</a>      | 6.0 | All | All | All |
| Operating System | <a href="#">Redhat</a> | <a href="#">Enterprise Linux Workstation</a> | 6.0 | All | All | All |
| Operating System | <a href="#">Redhat</a> | <a href="#">Enterprise Linux Workstation</a> | 6.0 | All | All | All |

## References

| Reference  | Source  | Link                 |
|--|---------|----------------------|
| Bug 2672 – ::1 can be spoofed. ACLs based on source IP can be bypassed   | CONFIRM | <a href="#">bug</a>  |
| Debian -- Security Information -- DSA-3388-1 ntp   | DEBIAN  | <a href="#">ww</a>   |
| Red Hat Customer Portal  | REDHAT  | <a href="#">rhn.</a> |
| Document Display   HPE Support Center  | CONFIRM | <a href="#">sup</a>  |
| Vulnerability Note VU#852879 - Network Time Protocol (NTP) Project NTP daemon (ntpd) contains multiple vulnerabilities | CERT-VN | <a href="#">ww</a>   |
| Oracle Linux Bulletin - October 2015   | CONFIRM | <a href="#">ww</a>   |
| Bug 1184572 – CVE-2014-9298 ntp: drop packets with source address ::1  | CONFIRM | <a href="#">bug</a>  |
| <a href="#">support.ntp.org/bin/view/Main/SecurityNotice</a>   | CONFIRM | <a href="#">sup</a>  |
| NTP 'ntp_io.c' Authentication Security Bypass Vulnerability  | BID     | <a href="#">ww</a>   |
| CVE Program record   | CVE.ORG | <a href="#">ww</a>   |
| NVD vulnerability detail   | NVD     | <a href="#">nvd</a>  |

No vendor comments have been submitted for this CVE.

## Legacy QID Mappings

[43837](#) HPE Comware 5 And Comware 7 Switches And Routers using NTP, Remote Denial Of Service (HPESBHF03886)

© [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](#)