



# CVE-2017-5202

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

## Summary

|                        |                                                                                                    |
|------------------------|----------------------------------------------------------------------------------------------------|
| <b>CVE</b>             | CVE-2017-5202                                                                                      |
| <b>State</b>           | PUBLIC                                                                                             |
| <b>Assigner</b>        | cve@mitre.org                                                                                      |
| <b>Source Priority</b> | CVE Program / NVD first with legacy fallback                                                       |
| <b>Published</b>       | 2017-01-28 01:59:00 UTC                                                                            |
| <b>Updated</b>         | 2023-11-07 02:49:00 UTC                                                                            |
| <b>Description</b>     | The ISO CLNS parser in tcpdump before 4.9.0 has a buffer overflow in print-isoclns.c:clnp_print(). |

## Risk And Classification

### Problem Types: CWE-119

## NVD Known Affected Configurations (CPE 2.3)

| Type             | Vendor                 | Product                                     | Version | Update | Edition | Language |
|------------------|------------------------|---------------------------------------------|---------|--------|---------|----------|
| 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>                | 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="#">Redhat</a> | <a href="#">Enterprise Linux Desktop</a>    | 7.0     | All    | All     | All      |
| Operating System | <a href="#">Redhat</a> | <a href="#">Enterprise Linux Desktop</a>    | 7.0     | All    | All     | All      |
| Operating System | <a href="#">Redhat</a> | <a href="#">Enterprise Linux Server</a>     | 7.0     | All    | All     | All      |
| Operating System | <a href="#">Redhat</a> | <a href="#">Enterprise Linux Server</a>     | 7.0     | All    | All     | All      |
| Operating System | <a href="#">Redhat</a> | <a href="#">Enterprise Linux Server Aus</a> | 7.4     | All    | All     | All      |
| Operating System | <a href="#">Redhat</a> | <a href="#">Enterprise Linux Server Aus</a> | 7.6     | All    | All     | All      |
| Operating System | <a href="#">Redhat</a> | <a href="#">Enterprise Linux Server Aus</a> | 7.4     | All    | All     | All      |
| Operating System | <a href="#">Redhat</a> | <a href="#">Enterprise Linux Server Aus</a> | 7.6     | All    | All     | All      |
| Operating System | <a href="#">Redhat</a> | <a href="#">Enterprise Linux Server Eus</a> | 7.4     | All    | All     | All      |
| Operating System | <a href="#">Redhat</a> | <a href="#">Enterprise Linux Server Eus</a> | 7.5     | All    | All     | All      |
| Operating System | <a href="#">Redhat</a> | <a href="#">Enterprise Linux Server Eus</a> | 7.6     | All    | All     | All      |
| Operating System | <a href="#">Redhat</a> | <a href="#">Enterprise Linux Server Eus</a> | 7.4     | All    | All     | All      |
| Operating System | <a href="#">Redhat</a> | <a href="#">Enterprise Linux Server Eus</a> | 7.5     | All    | All     | All      |

|                  |                         |                                              |     |     |     |     |
|------------------|-------------------------|----------------------------------------------|-----|-----|-----|-----|
| Operating System | <a href="#">Redhat</a>  | <a href="#">Enterprise Linux Server Eus</a>  | 7.6 | All | All | All |
| Operating System | <a href="#">Redhat</a>  | <a href="#">Enterprise Linux Server Tus</a>  | 7.6 | All | All | All |
| Operating System | <a href="#">Redhat</a>  | <a href="#">Enterprise Linux Server Tus</a>  | 7.6 | All | All | All |
| Operating System | <a href="#">Redhat</a>  | <a href="#">Enterprise Linux Workstation</a> | 7.0 | All | All | All |
| Operating System | <a href="#">Redhat</a>  | <a href="#">Enterprise Linux Workstation</a> | 7.0 | All | All | All |
| Application      | <a href="#">Tcpdump</a> | <a href="#">Tcpdump</a>                      | All | All | All | All |
| Application      | <a href="#">Tcpdump</a> | <a href="#">Tcpdump</a>                      | All | All | All | All |

## References

| Reference                                                                                         | Source   | Link                                                         |
|---------------------------------------------------------------------------------------------------|----------|--------------------------------------------------------------|
| Debian -- Security Information -- DSA-3775-1 tcpdump                                              | DEBIAN   | <a href="http://www.debian.org">www.debian.org</a>           |
| tcpdump: Multiple vulnerabilities (GLSA 201702-30) — Gentoo Security                              | GENTOO   | <a href="http://security.gentoo.org">security.gentoo.org</a> |
| Bug#852744: unblock: tcpdump/4.9.0-1                                                              |          | <a href="http://www.mail-archive.cc">www.mail-archive.cc</a> |
| Bug#852744: unblock: tcpdump/4.9.0-1                                                              | CONFIRM  | <a href="http://www.mail-archive.cc">www.mail-archive.cc</a> |
| tcpdump Multiple Buffer Overflow Vulnerabilities                                                  | BID      | <a href="http://www.securityfocus.c">www.securityfocus.c</a> |
| Tcpdump Multiple Flaws Let Remote Users Deny Service and Execute Arbitrary Code - SecurityTracker | SECTrack | <a href="http://www.securitytracker">www.securitytracker</a> |
| Red Hat Customer Portal                                                                           | REDHAT   | <a href="http://access.redhat.com">access.redhat.com</a>     |
| CVE Program record                                                                                | CVE.ORG  | <a href="http://www.cve.org">www.cve.org</a>                 |
| NVD vulnerability detail                                                                          | NVD      | <a href="http://nvd.nist.gov">nvd.nist.gov</a>               |

No vendor comments have been submitted for this CVE.

## Legacy QID Mappings

|                                                                                       |
|---------------------------------------------------------------------------------------|
| <a href="#">500684</a> Alpine Linux Security Update for tcpdump                       |
| <a href="#">504453</a> Alpine Linux Security Update for tcpdump                       |
| <a href="#">710418</a> Gentoo Linux tcpdump Multiple Vulnerabilities (GLSA 201702-30) |

© [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](#).

Free CVE JSON API [cve.report/api](http://cve.report/api)

CVE.report and Source URL Uptime Status [status.cve.report](http://status.cve.report)