



# CVE-2010-0624

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

## Summary

|                        |  |
|------------------------|--|
| <b>CVE</b>             | CVE-2010-0624  |
| <b>State</b>           | PUBLIC   |
| <b>Assigner</b>        | cve@mitre.org  |
| <b>Source Priority</b> | CVE Program / NVD first with legacy fallback   |
| <b>Published</b>       | 2010-03-15 13:28:00 UTC  |
| <b>Updated</b>         | 2018-10-10 19:53:00 UTC  |
| <b>Description</b>     | Heap-based buffer overflow in the rmt_read__ function in lib/rtapelib.c in the rmt client functionality in GNU tar before 1.23 |

## Risk And Classification

### Problem Types: CWE-119

## NVD Known Affected Configurations (CPE 2.3)

| Type        | Vendor | Product | Version | Update | Edition | Language |
|-------------|--------|---------|---------|--------|---------|----------|
| Application | Gnu    | Cpio    | 1.0     | All    | All     | All      |
| Application | Gnu    | Cpio    | 1.1     | All    | All     | All      |
| Application | Gnu    | Cpio    | 1.2     | All    | All     | All      |
| Application | Gnu    | Cpio    | 1.3     | All    | All     | All      |
| Application | Gnu    | Cpio    | 2.4-2   | All    | All     | All      |
| Application | Gnu    | Cpio    | 2.5     | All    | All     | All      |
| Application | Gnu    | Cpio    | 2.5.90  | All    | All     | All      |
| Application | Gnu    | Cpio    | 2.6     | All    | All     | All      |
| Application | Gnu    | Cpio    | 2.7     | All    | All     | All      |
| Application | Gnu    | Cpio    | 2.8     | All    | All     | All      |
| Application | Gnu    | Cpio    | 2.9     | All    | All     | All      |
| Application | Gnu    | Cpio    | 1.0     | All    | All     | All      |
| Application | Gnu    | Cpio    | 1.1     | All    | All     | All      |
| Application | Gnu    | Cpio    | 1.2     | All    | All     | All      |
| Application | Gnu    | Cpio    | 1.3     | All    | All     | All      |
| Application | Gnu    | Cpio    | 2.4-2   | All    | All     | All      |
| Application | Gnu    | Cpio    | 2.5     | All    | All     | All      |

|             |     |      |         |     |     |     |
|-------------|-----|------|---------|-----|-----|-----|
| Application | Gnu | Cpio | 2.5.90  | All | All | All |
| Application | Gnu | Cpio | 2.6     | All | All | All |
| Application | Gnu | Cpio | 2.7     | All | All | All |
| Application | Gnu | Cpio | 2.8     | All | All | All |
| Application | Gnu | Cpio | 2.9     | All | All | All |
| Application | Gnu | Cpio | All     | All | All | All |
| Application | Gnu | Tar  | 1.13    | All | All | All |
| Application | Gnu | Tar  | 1.13.11 | All | All | All |
| Application | Gnu | Tar  | 1.13.14 | All | All | All |
| Application | Gnu | Tar  | 1.13.16 | All | All | All |
| Application | Gnu | Tar  | 1.13.17 | All | All | All |
| Application | Gnu | Tar  | 1.13.18 | All | All | All |
| Application | Gnu | Tar  | 1.13.19 | All | All | All |
| Application | Gnu | Tar  | 1.13.25 | All | All | All |
| Application | Gnu | Tar  | 1.13.5  | All | All | All |
| Application | Gnu | Tar  | 1.14    | All | All | All |
| Application | Gnu | Tar  | 1.14.1  | All | All | All |
| Application | Gnu | Tar  | 1.14.90 | All | All | All |
| Application | Gnu | Tar  | 1.15    | All | All | All |
| Application | Gnu | Tar  | 1.15.1  | All | All | All |
| Application | Gnu | Tar  | 1.15.90 | All | All | All |
| Application | Gnu | Tar  | 1.15.91 | All | All | All |
| Application | Gnu | Tar  | 1.16    | All | All | All |
| Application | Gnu | Tar  | 1.16.1  | All | All | All |
| Application | Gnu | Tar  | 1.17    | All | All | All |
| Application | Gnu | Tar  | 1.18    | All | All | All |
| Application | Gnu | Tar  | 1.19    | All | All | All |
| Application | Gnu | Tar  | 1.20    | All | All | All |
| Application | Gnu | Tar  | 1.21    | All | All | All |
| Application | Gnu | Tar  | 1.13    | All | All | All |
| Application | Gnu | Tar  | 1.13.11 | All | All | All |
| Application | Gnu | Tar  | 1.13.14 | All | All | All |
| Application | Gnu | Tar  | 1.13.16 | All | All | All |
| Application | Gnu | Tar  | 1.13.17 | All | All | All |
| Application | Gnu | Tar  | 1.13.18 | All | All | All |

|             |     |     |         |     |     |     |
|-------------|-----|-----|---------|-----|-----|-----|
| Application | Gnu | Tar | 1.13.19 | All | All | All |
| Application | Gnu | Tar | 1.13.25 | All | All | All |
| Application | Gnu | Tar | 1.13.5  | All | All | All |
| Application | Gnu | Tar | 1.14    | All | All | All |
| Application | Gnu | Tar | 1.14.1  | All | All | All |
| Application | Gnu | Tar | 1.14.90 | All | All | All |
| Application | Gnu | Tar | 1.15    | All | All | All |
| Application | Gnu | Tar | 1.15.1  | All | All | All |
| Application | Gnu | Tar | 1.15.90 | All | All | All |
| Application | Gnu | Tar | 1.15.91 | All | All | All |
| Application | Gnu | Tar | 1.16    | All | All | All |
| Application | Gnu | Tar | 1.16.1  | All | All | All |
| Application | Gnu | Tar | 1.17    | All | All | All |
| Application | Gnu | Tar | 1.18    | All | All | All |
| Application | Gnu | Tar | 1.19    | All | All | All |
| Application | Gnu | Tar | 1.20    | All | All | All |
| Application | Gnu | Tar | 1.21    | All | All | All |
| Application | Gnu | Tar | All     | All | All | All |

## References

| Reference  | Source   | L  |
|--|----------|----|
| Support / Security / Advisories // MDVSA-2010:065   Mandriva     | MANDRIVA | v  |
| Webmail : Solution de messagerie professionnelle - OVHcloud- OVH | VUPEN    | v  |
| Repository / Oval Repository                                     | OVAL     | c  |
| Webmail - OVH  | VUPEN    | v  |
| Red Hat update for tar - Secunia.com                             | SECUNIA  | s  |
| Webmail : Solution de messagerie professionnelle - OVHcloud- OVH | VUPEN    | v  |
| [SECURITY] Fedora 11 Update: tar-1.22-5.fc11                     | FEDORA   | li |
| Support  | REDHAT   | v  |
| GNU Cpio "rmt" Buffer Overflow Vulnerability - Secunia.com       | SECUNIA  | s  |
| Support  | REDHAT   | v  |
| [SECURITY] Fedora 12 Update: cpio-2.10-5.fc12                    | FEDORA   | li |
| [SECURITY] Fedora 11 Update: cpio-2.9.90-8.fc11                  | FEDORA   | li |
| SecurityFocus  | BUGTRAQ  | v  |
| Fedora update for cpio - Secunia.com                             | SECUNIA  | s  |
| Webmail : Solution de messagerie professionnelle - OVHcloud- OVH | VUPEN    | v  |

|   |         |    |
|---|---------|----|
| Repository / Oval Repository  | OVAL    | c  |
| [SECURITY] Fedora 12 Update: tar-1.22-12.fc12   | FEDORA  | li |
| Webmail - OVH   | VUPEN   | v  |
| Gentoo Linux Documentation -- GNU Tar: User-assisted execution of arbitrary code                                      | GENTOO  | s  |
| [security-announce] SUSE Security Summary Report: SUSE-SR:2010:011  | SUSE    | li |
| Fedora 12 Update: cpio-2.10-4.fc12  | FEDORA  | li |
| 62950   | OSVDB   | c  |
| 564368 – (CVE-2010-0624) CVE-2010-0624 tar, cpio: Heap-based buffer overflow by expanding a specially-crafted archive | CONFIRM | t  |
| AG Rechnersicherheit: GNU tar/cpio  | MISC    | v  |
| Support   | REDHAT  | v  |
| Webmail : Solution de messagerie professionnelle - OVHcloud- OVH  | VUPEN   | v  |
| issues.rpath.com/browse/RPL-3219  | CONFIRM | is |
| Webmail : Solution de messagerie professionnelle - OVHcloud- OVH  | VUPEN   | v  |
| Support   | REDHAT  | v  |
| Juniper Networks - 2015-10 Security Bulletin: CTPView: Multiple Vulnerabilities in CTPView                            | CONFIRM | k  |
| USN-2456-1: GNU cpio vulnerabilities   Ubuntu   | UBUNTU  | v  |
| 2015-07 Security Bulletin: CTPView: Multiple vulnerabilities in CTPView - Juniper Networks                            | CONFIRM | k  |
| CVE Program record  | CVE.ORG | v  |
| NVD vulnerability detail  | NVD     | r  |

No vendor comments have been submitted for this CVE.

There are currently no legacy QID mappings associated with this CVE.

© [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](#)