



# CVE-2013-4397

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

## Summary

<b>CVE</b>	CVE-2013-4397
<b>State</b>	PUBLIC
<b>Assigner</b>	secalert@redhat.com
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2013-10-17 23:55:00 UTC
<b>Updated</b>	2023-02-13 04:46:00 UTC
<b>Description</b>	Multiple integer overflows in the th_read function in lib/block.c in libtar before 1.2.20 allow remote attackers to cause a denial of service.

## Risk And Classification

**Problem Types:** CWE-189

## NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	<a href="#">Feep</a>	<a href="#">Libtar</a>	1.2.11	All	All	All
Application	<a href="#">Feep</a>	<a href="#">Libtar</a>	1.2.13	All	All	All
Application	<a href="#">Feep</a>	<a href="#">Libtar</a>	1.2.14	All	All	All
Application	<a href="#">Feep</a>	<a href="#">Libtar</a>	1.2.15	All	All	All
Application	<a href="#">Feep</a>	<a href="#">Libtar</a>	1.2.16	All	All	All
Application	<a href="#">Feep</a>	<a href="#">Libtar</a>	1.2.17	All	All	All
Application	<a href="#">Feep</a>	<a href="#">Libtar</a>	1.2.18	All	All	All
Application	<a href="#">Feep</a>	<a href="#">Libtar</a>	1.2.11	All	All	All
Application	<a href="#">Feep</a>	<a href="#">Libtar</a>	1.2.13	All	All	All
Application	<a href="#">Feep</a>	<a href="#">Libtar</a>	1.2.14	All	All	All
Application	<a href="#">Feep</a>	<a href="#">Libtar</a>	1.2.15	All	All	All
Application	<a href="#">Feep</a>	<a href="#">Libtar</a>	1.2.16	All	All	All
Application	<a href="#">Feep</a>	<a href="#">Libtar</a>	1.2.17	All	All	All
Application	<a href="#">Feep</a>	<a href="#">Libtar</a>	1.2.18	All	All	All
Application	<a href="#">Feep</a>	<a href="#">Libtar</a>	All	All	All	All
Operating System	<a href="#">Redhat</a>	<a href="#">Enterprise Linux</a>	6.0	All	All	All
Operating System	<a href="#">Redhat</a>	<a href="#">Enterprise Linux</a>	6.0	All	All	All

## References

Reference	Source
Public Git Hosting - libtar.git/commitdiff	CONFID
Red Hat Customer Portal	MISC
Google Android Bugs Let Remote Users Obtain Sensitive Information, Deny Service, and Execute Arbitrary Code - SecurityTracker	SECTR
CVE-2013-4397 - Red Hat Customer Portal	MISC
Security Advisory SA55188 - libtar GNU Long Name and Long Link Extensions Two Integer Overflow Vulnerabilities - Secunia	SECUN
libtar Integer Overflow Lets Remote Users Execute Arbitrary Code - SecurityTracker	SECTR
oss-security - Integer overflow in libtar (<= 1.2.19)	MLIST
Red Hat Customer Portal	REDHA
Malformed Request	BID
1014492 – (CVE-2013-4397) CVE-2013-4397 libtar: Heap-based buffer overflows by expanding a specially-crafted archive	MISC
Debian -- Security Information -- DSA-2817-1 libtar	DEBIAN
Android Security Bulletin—January 2018   Android Open Source Project	CONFID
Security Advisory SA55253 - Red Hat update for libtar - Secunia	SECUN
[libtar] 20131009 ANNOUNCE: libtar version 1.2.20	MLIST
oss-security - Re: Integer overflow in libtar (<= 1.2.19)	MLIST
CVE Program record	CVE.OP
NVD vulnerability detail	NVD

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](#)