



CVE-2017-14122

[MITRE](#)[NVD](#)[CVE.ORG](#)[Print: PDF !\[\]\(e3f8612927870f2e0f9f5989e6dd3064_img.jpg\)](#)

Summary

CVE	CVE-2017-14122
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2017-09-03 20:29:00 UTC
Updated	2021-02-25 17:17:00 UTC
Description	unrar 0.0.1 (aka unrar-free or unrar-gpl) suffers from a stack-based buffer over-read in unrarlib.c, related to ExtrFile and stri

Risk And Classification

Problem Types: CWE-125

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Debian	Debian Linux	9.0	All	All	All
Operating System	Debian	Debian Linux	9.0	All	All	All
Application	Rarlab	Unrar	0.0.1	All	All	All
Application	Rarlab	Unrar	0.0.1	All	All	All

References

Reference	Source	Link	Tags
[SECURITY] [DLA 2567-1] unrar-free security update	MLIST	lists.debian.org	Mailing Lis
oss-security - unrar-free/unrar-gpl: directory traversal and other issues	MISC	www.openwall.com	Mailing Lis
#874060 - unrar-free: CVE-2017-14122: stack overread vulnerability - Debian Bug report logs	MISC	bugs.debian.org	Issue Trac
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical,

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](#)