

# CVE-2022-30333

## RARLAB UnRAR Directory Traversal Vulnerability

CISA KEV since Aug 9, 2022

Actively exploited

Ransomware use known

Public exploit module (Metasploit)

RARLAB UnRAR before 6.12 on Linux and UNIX allows directory traversal to write to files during an extract (aka unpack) operation, as demonstrated by creating a ~/.ssh/authorized\_keys file. NOTE: WinRAR and Android RAR are unaffected.

|                                                            |                                              |                                                           |                                                                                    |
|------------------------------------------------------------|----------------------------------------------|-----------------------------------------------------------|------------------------------------------------------------------------------------|
| <b>EVRS</b><br><b>90</b> /100<br><b>Immediate</b> priority | <b>CVSS V3.1</b><br><b>7.5</b><br>High · NVD | <b>EPSS</b><br><b>0.992</b><br>99.94th percentile · FIRST | <b>CISA DEADLINE</b><br><b>Aug 30, 2022</b><br>KEV since 2022 · listed over a year |
|------------------------------------------------------------|----------------------------------------------|-----------------------------------------------------------|------------------------------------------------------------------------------------|

### Signals behind the score

☒ counted in the score ☐ not counted

evidence for 6 of 8 signals

|                                                       |                            |                                                                |                                            |
|-------------------------------------------------------|----------------------------|----------------------------------------------------------------|--------------------------------------------|
| <input checked="" type="checkbox"/> <b>CISA KEV</b>   | Listed in the catalog      | <input type="checkbox"/> <b>Vendor exploitation</b>            | Confirmed exploitation in the wild         |
| <input checked="" type="checkbox"/> <b>Ransomware</b> | Known ransomware campaigns | <input type="checkbox"/> <b>KEV recency</b>                    | On the CISA KEV catalog for over two years |
| <input checked="" type="checkbox"/> <b>EPSS</b>       | 0.992 probability          | <input type="checkbox"/> <b>Pre-patch disclosure</b>           | Disclosure status unavailable              |
| <input checked="" type="checkbox"/> <b>CVSS</b>       | Base score 7.5             | <input type="checkbox"/> <b>Microsoft Exploitability Index</b> | Not a Microsoft CVE                        |

### Remediation

**Patch Immediately** Patch or fixed version identified

**CISA required action:** Apply updates per vendor instructions. **CISA note:** Vulnerability updated with version 6.12.  
Basis: CISA KEV required action

### Affected and fixed versions

| PACKAGE      | AFFECTED | FIXED IN                | SOURCE |
|--------------|----------|-------------------------|--------|
| unrar        | < 6.12   | no fixed version listed | NVD    |
| linux kernel | —        | no fixed version listed | NVD    |
| unix         | —        | no fixed version listed | NVD    |
| debian linux | 10.0     | no fixed version listed | NVD    |

### Sources

**Vendor guidance** [rarlab.com/rar/rarlinux-x32-612.tar.gz](https://rarlab.com/rar/rarlinux-x32-612.tar.gz)  
**NVD** [nvd.nist.gov/vuln/detail/CVE-2022-30333](https://nvd.nist.gov/vuln/detail/CVE-2022-30333)

**Additional guidance** [security.gentoo.org/glsa/202309-04](https://security.gentoo.org/glsa/202309-04)  
**CISA KEV** [cisa.gov/known-exploited-vulnerabilities-catalog](https://cisa.gov/known-exploited-vulnerabilities-catalog)  
**Current data** [evulnable.com/vulnerability-management/cve/CVE-2022-30333](https://evulnable.com/vulnerability-management/cve/CVE-2022-30333)

**ENISA EUVD** [euvd.enisa.europa.eu/vulnerability/EUVD-2022-52276](https://euvd.enisa.europa.eu/vulnerability/EUVD-2022-52276)

Snapshot at generation time. EPSS can move quickly. A public exploit module is not evidence of active exploitation.