



Tar: tar: hidden file injection via crafted archives

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

Summary

CVE	CVE-2026-5704
State	PUBLISHED
Assigner	redhat
Source Priority	CVE Program / NVD first with legacy fallback
Published	2026-04-06 16:16:42 UTC
Updated	2026-04-06 16:16:42 UTC
Description	A flaw was found in tar. A remote attacker could exploit this vulnerability by crafting a malicious archive, leading to hidden fi

Risk And Classification

Primary CVSS: v3.1 5 MEDIUM from secalert@redhat.com

CVSS:3.1/AV:L/AC:L/PR:L/UI:R/S:U/C:N/I:H/A:N

Problem Types: CWE-434 | CWE-434 Unrestricted Upload of File with Dangerous Type

Version	Source	Type	Score	Severity	Vector
3.1	secalert@redhat.com	Primary	5	MEDIUM	CVSS:3.1/AV:L/AC:L/PR:L/UI:R/S:U/C:N/I:H/A:N
3.1	CNA	CVSS	5	MEDIUM	CVSS:3.1/AV:L/AC:L/PR:L/UI:R/S:U/C:N/I:H/A:N

CVSS v3.1 Breakdown

Attack Vector

Local

Attack Complexity

Low

Privileges Required

Low

User Interaction

Required

Scope

Unchanged

Confidentiality

None

Integrity

High

Availability

None

CVSS:3.1/AV:L/AC:L/PR:L/UI:R/S:U/C:N/I:H/A:N

Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	Red Hat	Red Hat Enterprise Linux 10	Not specified	Not specified
CNA	Red Hat	Red Hat Enterprise Linux 6	Not specified	Not specified
CNA	Red Hat	Red Hat Enterprise Linux 7	Not specified	Not specified
CNA	Red Hat	Red Hat Enterprise Linux 8	Not specified	Not specified
CNA	Red Hat	Red Hat Enterprise Linux 9	Not specified	Not specified

References

Reference	Source	Link	Tags
bugzilla.redhat.com/show_bug.cgi	secalert@redhat.com	bugzilla.redhat.com	
access.redhat.com/security/cve/CVE-2026-5704	secalert@redhat.com	access.redhat.com	
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical, analysis

Vendor Comments And Credit

Discovery Credit

CNA: Red Hat would like to thank Guillermo de Angel Garcia for reporting this issue. (en)

Additional Advisory Data

Source	Time	Event
CNA	2026-04-06T13:36:20.000Z	Reported to Red Hat.
CNA	2026-04-06T13:36:20.000Z	Made public.

Workarounds

CNA: To mitigate this issue, avoid extracting archives from untrusted sources. If processing untrusted archives is necessary, do so within a sandboxed environment to limit potential impact.

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

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](#)