Bug 2455360 (CVE-2026-5704) - CVE-2026-5704 tar: tar: Hidden file injection via crafted archives

Keywords: Security

Status: NEW

Alias: CVE-2026-5704

Product: Security Response

Component: vulnerability

Version: unspecified

Hardware: All

OS: Linux

Priority: medium

Severity: medium

Target Milestone: ---

Assignee: Product Security DevOps Team

QA Contact:

Docs Contact:

URL:

Whiteboard:

Depends On:

Blocks:

TreeView+ depends on / blocked

Reported: 2026-04-06 13:38 UTC by OSIDB Bzimport

Modified: 2026-04-06 15:10 UTC (History)

CC List: 0 users

Fixed In Version:

Clone Of:

Environment:

Last Closed:

Embargoed:

Attachments (Terms of Use)

OSIDB Bzimport 2026-04-06 13:38:08 UTC Description

```
Summary:
GNU tar allows malformed archives where non-data-bearing
typeflags (symlink, char device, block device, FIFO) contain a
non-zero size field, leading to inconsistent behavior between
listing (tar -t) and extraction (tar -x). This results in
stream desynchronization and enables hidden file injection.
Requirements to exploit:
An attacker only needs the ability to supply a crafted tar
archive to a target system that performs pre-extraction
inspection using tar -t (or equivalent API) and later extracts
it using GNU tar. No privileges or user interaction beyond
extraction are required.

Patch Available:
```

no

Version Fixed:
N/A

Impact:
Hidden file injection with fully attacker-controlled content

Bypass of pre-extraction inspection mechanisms

Single-implementation inconsistency (no cross-tool pipeline required)

Attack complexity: Low (crafted archive is < 3 KB, no special privileges)

Affected typeflags: '2', '3', '4', '6' (4 of 5 non-data typeflags)

Steps to reproduce if available:

Generate a crafted archive with a non-data-bearing typeflag (e.g., chardev) and non-zero size.

List contents

```
tar -tf crafted.tar
```

→ injected file is NOT shown

Extract archive:

```
tar -xf crafted.tar
```

Observe additional file created on disk that was not present in listing output.

Note

You need to log in before you can comment on or make changes to this bug.