



## Bug 2439040 (CVE-2026-26158) - CVE-2026-26158 busybox: BusyBox: Arbitrary file modification and privilege escalation via unvalidated tar archive entries

**Keywords:** Security

**Reported:** 2026-02-11 18:13 UTC by OSIDB Bzimport

**Status:** NEW

**Modified:** 2026-02-11 20:18 UTC ([History](#))

**Alias:** CVE-2026-26158

**CC List:** 14 users ([show](#))

**Product:** Security Response

**Fixed In Version:**

**Component:** vulnerability

**Clone Of:**

**Environment:**

**Version:** unspecified

**Last Closed:**

**Embargoed:**

**Hardware:** All

**OS:** Linux

**Priority:** high

**Severity:** high

**Target Milestone:** ---

**Assignee:** Product Security DevOps Team

**QA Contact:**

**Docs Contact:**

**URL:**

**Whiteboard:**

**Depends On:** [2439048](#) [2439049](#) [2439050](#)

**Blocks:**

**TreeView+** [depends on](#) / [blocked](#)

**Attachments** ([Terms of Use](#))

OSIDB Bzimport 2026-02-11 18:13:37 UTC

[Description](#)

Affects: BusyBox v1.36.1 and v1.37.0 (likely affects earlier versions too)  
CVSS: 9.3 (CRITICAL)  
Component: data\_extract\_all.c in tar extraction - hardlink and symlink handling

Description:  
Hardlink entries in tar archives are created without validation of the link\_target path. This allows modification of files outside the extraction directory and bypasses existing path traversal mitigations.

This vulnerability has higher impact than the path traversal issue as it does not rely on relative paths or the current working directory.

Technical Details:

- Hardlink entries can point to absolute paths like /etc/passwd
- Symlink entries suffer from the same root cause (missing link\_target validation)
- When extraction is performed with elevated privileges, attackers can modify critical system files

Impact:

Arbitrary file modification outside extraction directory, privilege escalation when combined with elevated extraction permissions, bypass of path traversal protections.

Note: While hardlinks and symlinks share the same root cause (missing link\_target validation), I'm requesting a single CVE for this issue.

---

Note

You need to [log in](#) before you can comment on or make changes to this bug.

