



Bug 2439039 (CVE-2026-26157) - CVE-2026-26157 busybox: BusyBox: Arbitrary file overwrite and potential code execution via incomplete path sanitization

Keywords: Security

Reported: 2026-02-11 18:09 UTC by OSIDB Bzimport

Status: NEW

Modified: 2026-02-11 20:17 UTC ([History](#))

Alias: CVE-2026-26157

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: [2439044](#) [2439045](#) [2439046](#)

Blocks:

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

Attachments ([Terms of Use](#))

OSIDB Bzimport 2026-02-11 18:09:04 UTC

[Description](#)

Affects: BusyBox v1.36.1 and v1.37.0 (likely affects earlier versions too)
CVSS: 8.6 (HIGH)
Component: strip_unsafe_prefix() function in archive extraction utilities
(tar, unzip, rpm, ar, dpkg)

Description:
Incomplete path sanitization fails to detect trailing ".." components in filenames (e.g., "logs/data/.."), allowing files to be written outside the intended extraction directory when the current working

directory matches the target location. An attacker can craft malicious archives that overwrite arbitrary files within the extraction directory scope.

Impact:

Arbitrary file overwrite, potential code execution through modification of shell configuration files, cron jobs, or other sensitive files.

Note

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

