Vim tabpanel modeline escape affects Vim < 9.2.0272

High **chrisbra** published **GHSA-2gmj-rpqf-pxvh** yesterday

Package	Affected versions	Patched versions
Vim	< 9.2.0172	9.2.0172

Severity

High 8.2 / 10

CVSS v3 base metrics

Attack vector	Local
Attack complexity	Low
Privileges required	None
User interaction	Required
Scope	Changed
Confidentiality	High
Integrity	High
Availability	None

Learn more about base metrics

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

CVE ID

CVE-2026-34714

Weaknesses

▶ CWE-78

Description

Vim tabpanel modeline escape affects Vim < 9.2.0272

Date: 30.03.2026
Severity: High
CVE: *not-yet-assigned*
CWE: Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection') (CWE-78)

Summary

A bug chain in Vim allows arbitrary OS command execution when a user opens
a crafted file. The `tabpanel` option is missing the `P_MLE` flag, allowing a modeline to inject a `%{expr}` expression string without requiring `modelineexpr` to be enabled. Although Vim correctly evaluates the expression
inside the sandbox, `autocmd_add()` lacks a `check_secure()` call, allowing sandboxed code to register an autocommand that fires after the sandbox exits.

Description

The `tabpanel` option (`src/optiondefs.h:2581`) accepts `%{expr}` format strings identically to `statusline` and `tabline` , both of which carry the `P_MLE` flag to require `modelineexpr` for modeline use. `tabpanel` is missing this flag, so the modeline security check at `src/option.c:1572-1576` is never reached and arbitrary expression strings are accepted from modelines.

Vim correctly detects that the option was set insecurely and evaluates the expression inside the sandbox (`src/eval.c:747-758`). However, `autocmd_add()` (`src/autocmd.c:3316`) contains no `check_secure()` call. While the `:autocmd` ex command is properly blocked in the sandbox (no `EX_SBOXOK`),
but the function interface bypasses this restriction.

Impact

An attacker who can deliver a crafted file to a victim achieves arbitrary command execution with the privileges of the user running Vim. The attack requires only that the victim opens the file; no further interaction is needed. `modeline` is enabled by default and `modelineexpr` does not need to be enabled. Vim builds with `+tabpanel` (FEAT_HUGE, the default) are affected.

Acknowledgements

The Vim project would like to thank Hung Nguyen for identifying the vulnerability
chain, providing a detailed root cause analysis, reproduction steps, and suggested fixes.

References

The issue has been fixed as of Vim patch v9.2.0272

- Commit
- GitHub Advisory