Message-ID: <aco9Ai89pj+OQ0YS@256bit.org>
Date: Mon, 30 Mar 2026 11:06:10 +0200
From: Christian Brabandt <cb@...bit.org>
To: oss-security@...ts.openwall.com
Subject: [vim-security] Vim tabpanel modeline escape affects Vim < 9.2.0272

```
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 (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 Koda Reef 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](https://github.com/vim/vim/releases/tag/v9.2.0272)

- [Commit](https://github.com/vim/vim/commit/664701eb7576edb7c7c7d9f2d600815ec1f43459)
- [GitHub Advisory](https://github.com/vim/vim/security/advisories/GHSA-2gmj-rpqf-pxvh)


Thanks,
Christian
--
Eine Diktatur ist ein Staat, in dem das Halten von Papageien mit
Lebensgefahr verbunden ist.
                -- Jack Lemmon
```