Your Linux system can be hacked just by opening a file in Vim or Neovim Editor

If you haven't updated your Linux operating system recently, especially the command line text editor, don't even try to access the contents of the file via Vim or Neovim, pay attention, your system is complete All can be hacked.

Linux users, be careful!

If you haven't updated your Linux operating system recently, especially the command line text editor, don't even try to access the contents of the file via Vim or Neovim, pay attention, your system is complete All can be hacked.

Well-known security researcher Armin Razmjou recently discovered a serious vulnerability related to executing arbitrary operating system commands (CVE-2019-12735) in Vim and Neovim - 2 line text editing applications The most common and powerful commands are usually preinstalled on most Linux-based operating systems.

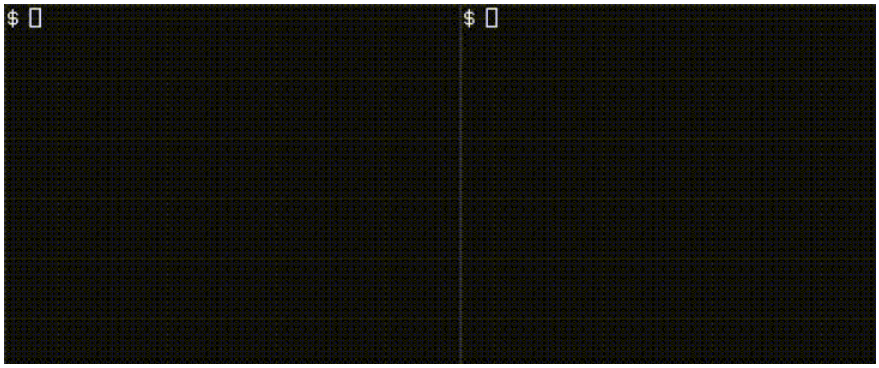
1. The Russian army will completely replace Windows with Astra Linux

On Linux systems, the Vim editor allows users to create, view or edit any file, including text, programming scripts and documents.

Because Neovim is just an extended version of Vim (with better user experience, plugins and GUI), of course the above serious code execution vulnerability will also appear in this application.

Vulnerabilities execute code in Vim and Neovim

Security expert Armin Razmjou has discovered a flaw in the way Vim editor handles "modelines" - the feature is turned on by default to automatically find and apply a set of customized options. Accessed by the file creator, close to the start and end lines in the document.

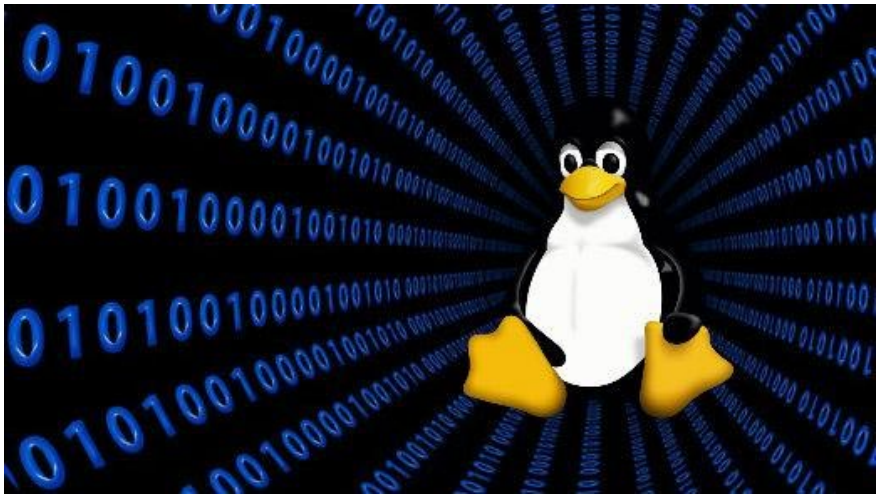


1. The Korean government is going to use the Linux operating system instead of Windows because of the expensive cost

Although the editor only allows applying a subset of options in the model (for security reasons) and using sandbox protection if it contains unsafe expressions, Armin Razmjou reveals that use the ": source!" (with an amendment [!]) can overcome sandbox protection.

Therefore, users who only need to open a specially crafted file using Vim or Neovim can also allow an attacker to secretly execute commands on their Linux system, as well as control the system. Remote system.

The security researcher has also released 2 Proof of Concept (PoC) on how to exploit the vulnerability mentioned above. One of these represents a real-life attack scenario when a remote attacker has access to the reverse shell from the victim's system as soon as he opens it.



1. Hacker successfully stole 100,000 photos from border control database

Developers responsible for maintenance of Vim (patch version 8.1.1365) and Neovim (released in v0.3.6) have also released updates for both of these utilities to solve the problem. Also recommend that users install the new version as soon as possible.

Besides, researcher Armin Razmjou has also provided some additional recommendations for users as follows:

1. Disable modelines feature
2. disable "modelineexpr" to not allow expressions to appear in modelines.
3. Switch to using the "securemodelines plugin" as a safe alternative to Vim models.

You finished reading the article "**Your Linux system can be hacked just by opening a file in Vim or Neovim Editor**" edited by the **TipsMake** team. We hope this article has provided you with many useful tech tips and tricks. You can search for similar articles on tips and guides. Thank you for reading and for following us regularly.
