

Plugins on well-known editing tools can give hackers priority

These tools are often extended with third-party plugins, but they often bring unpredictable dangers.

Whether a programmer or a writer, an editor always helps you work more effectively in a digital environment. For example, Sublime is used by many users due to its useful syntax highlighting and auto-complete tools.

These tools are often extended with third-party plugins. But these plugins often bring unpredictable dangers, even though plugins of familiar tools like Wordpress or Chrome.

Researcher at SafeBreach Dor Azouri analyzed some of the famous editing tools on Unix systems, Linux such as Sublime, Vim, Emacs, Gedit and pico / nano. Except for pico / nano, all have vulnerabilities that can help attackers escalate privileges and run malicious code.



Plugin from 3rd party is always hidden many dangers

This error lies in the stage when these tools download the plugin. Accordingly, the division of normal and escalating modes is not appropriately divided. The integrity of directory access is not preserved, so it is open to attackers with normal access to escalate privileges and run malicious code.

A simple malicious advertising campaign can help spread, run malicious code, install malware and completely control remote victim machines. Azouri recommends using open source host intrusion detection system named OSSEC to monitor system activity, logs, processes .

Users should avoid downloading 3rd party plugins while in Elevated mode and deny access to unprivileged users. Directory permissions, files should also be clearly divided between the two modes.

See more:

1. WordPress plugins with more than 300,000 pages that use vulnerabilities are vulnerable to SQL Injection attacks
2. How to remove and disable Plug-ins in the browser?
3. Visual Studio Code now has an extremely useful color picker

You finished reading the article "**Plugins on well-known editing tools can give hackers priority**" 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.