

How The Linux Foundation and Fedora are Addressing Workstation Security

By *srlinuxx*

Created 15/02/2013 - 9:44pm

Submitted by srlinuxx on Friday 15th of February 2013 09:44:49 PM Filed under [Linux](#) [1]

Are you a systems administrator? Quick, which system in your infrastructure is most vulnerable to hacker attacks? No, it's not the web server -- though it's a good guess. No, it's not the firewall. The answer may surprise you -- it's your workstation.

Think about it -- unless you're working for an agency with extremely rigid security policies, you are probably able to connect to servers you administer right from your workstation. Perhaps not all the time -- perhaps you have to establish a VPN connection first in order to be on the "inside." Once that is done, however, your workstation becomes an extremely interesting target for malicious hackers, since at that time your workstation happens to be the least protected system that sits both on the outside and on the inside of your trusted network.

Did you know that your workstation is currently running software that was written for the sole purpose of letting others execute arbitrary code?

[rest here](#) [2]

[Linux](#)

Source URL: <http://www.tuxmachines.org/node/59638>

Links:

[1] <http://www.tuxmachines.org/taxonomy/term/63>

[2] <http://www.linux.com/news/featured-blogs/203-konstantin-ryabitsev/699697-how-the-linux-foundation-and-fedora-are-addressing-workstation-security>