How To: Enable Password-less SUDO.

This isn’t the smartest thing you can do. In fact, you probably shouldn’t do this. But, if you are comfortable with your physical security, you can use sudo without a password.

In my case, there’s not a whole lot folks are going to do with sudo on my computer. Anyone with physical access to my device is someone that I trust. I also run a ton of commands when hanging out in the support sites and I am frankly just tired of typing my password when I use sudo.

So, let’s get rid of it. Start by pressing CTRL + ALT + T, and then enter:

[code]sudo nano /etc/sudoers[/code]

Scroll down to the bottom and add this line:

[code]<your_username> ALL=(ALL) NOPASSWD:ALL[/code]

Where “<your_username>” substitute it with your actual username on your computer. Now save it with:

CTRL + X

Y

ENTER

See that? You also may have just learned how use ‘nano’ to edit and save a text file while in the terminal. Pretty neat, huh? Anyhow, scroll up a little and look to the right. There’s a spot where you can enter a name and email address. If you do that (and confirm the email address) then you’ll get handy notices in the email when there’s a new article. I promise, I won’t send you a single non-site related email – ever.

USN-4741-1: Jackson vulnerabilities

It was discovered that Jackson Databind incorrectly handled deserialization. An attacker could possibly use this issue to execute
arbitrary code.

USN-4740-1: Apache Shiro vulnerabilities

It was discovered that Apache Shiro mishandled specially crafted requests. An
attacker could use this vulnerability to bypass authentication mechanisms.

USN-4739-1: WebKitGTK vulnerability

A large number of security issues were discovered in the WebKitGTK Web and
JavaScript engines. If a user were tricked into viewing a malicious
website, a remote attacker could exploit a variety of issues related to web
browser security, including cross-site scripting attacks,

denial of service
attacks, and arbitrary code execution.

USN-4738-1: OpenSSL vulnerabilities

Paul Kehrer discovered that OpenSSL incorrectly handled certain input
lengths in EVP functions. A remote attacker could possibly use this issue
to cause OpenSSL to crash, resulting in a denial of service.
(CVE-2021-23840)
Tavis Ormandy discovered that OpenSSL incorrectly handled parsing issuer
fields. A remote attacker could possibly use this issue to cause OpenSSL to
crash, resulting in a denial of service. (CVE-2021-23841)