USN-4735-1: PostgreSQL vulnerability

Heikki Linnakangas discovered that PostgreSQL incorrectly leaked values of
denied columns when handling certain errors. A remote attacker could
possibly use this issue to obtain sensitive information.

How To: Enable Root User In Ubuntu

This article is just a really simple article. In it, I'm going to tell you how to enable the root account in Ubuntu (and related derivatives) by assigning a password to the account.

First, if I may, I'd like to express some displeasures.

If you were to go ask this question on a number of sites, the people there would treat you as though you were a leper or a child. They'll respond with things like, "You don't need to use the root account, that's what sudo is for." Then, they'll helpfully link you to a long-winded explanation of why using sudo is better.

Truth be told, they're correct. They're right. You shouldn't be using the root account when it can be avoided — and it can pretty much always be avoided.

But, it demonstrates one of my pet peeves. See, they didn't answer the question. It doesn't matter that doing so may cause you untold horrors. What matters is that you asked a question and they opted to not answer you. It shouldn't matter to them

that you're gonna do something stupid. What should matter to them is giving you the answer to your damned question!

So, when someone asks me how to enable the root account — I tell them. Of course, I also mention that doing so is absolutely a bad idea, but I actually answer the question. This applies to other questions. If you ask a question, I do my best to answer it — if I am indeed taking the time to answer it. Maybe you just want to know how to do something? Maybe you have a good reason for it? It doesn't matter to me, I answer the question to the best of my ability. Included in that is the appropriate warning, but I at least answer the question.

Linux is about freedom, and that freedom should include doing things that go against the grain. That freedom should include doing things like hosing your operating system. That freedom should include doing the 'wrong' things and doing them the 'wrong' way.

So, keep that in mind when you're answering questions — and not just this specific question. The person asking the question should get a real answer to their question, even if they're asking the wrong question. If you can see it's an X-Y problem, ask them for more information — but don't be snide or aloof. If you're not going to answer the question, just click that X in the upper right corner and close the tab. Sure, give them a warning — but also give them an answer.

So, on that note, here's how you enable the root account in Ubuntu and distros derived from Ubuntu.

CTRL + ALT + T to open your terminal and enter:

[code]sudo passwd root[/code]

Now, don't get confused, it's going to ask you for *your* password. Enter that, your normal account password, and press the enter button.

Next, it's going to ask you to enter your new password for root. So, type that in and press enter. Then, it's going to ask you to type that same password again, and again you'll press enter when you're done.

That's it. Root is now enabled and you could login as root via TTY (this does not allow you to login as root via the GUI login during boot, that's for a different article) or whatnot. You just probably shouldn't. See, root has access to everything. It's a security risk and it's increasing the likelihood that you'll irrevocably ruin your operating system when you fat-finger a command. Seriously, don't do this. It's just a bad idea and you can easily use 'sudo'.

Like always, thanks for reading. Look to the right sidebar and enter a name and email address. That way, you'll know when I publish something! You want to know that, don't you?

Linux Foundation Newsletter February 2021: IT Training & Certification Sale, Shuah Khan & Mentorship, OpenSSF First Six Months

Click here to read the February 2021 Linux Foundation Newsletter

The post Linux Foundation Newsletter February 2021: IT Training & Certification Sale, Shuah Khan & Mentorship, OpenSSF First Six Months appeared first on Linux Foundation.

USN-4734-1: wpa_supplicant and hostapd vulnerabilities

It was discovered that wpa_supplicant did not properly handle P2P
(Wi-Fi Direct) group information in some situations, leading to a
heap overflow. A physically proximate attacker could use this to cause a
denial of service or possibly execute arbitrary code.
(CVE-2021-0326)
It was discovered that hostapd did not properly handle UPnP subscribe
messages in some circumstances. An attacker could use this to cause a
denial of service. (CVE-2020-12695)

How To: Check Your Logs For Errors

When you notice a problem with your Linux box, you're possibly only noticing the symptoms and not actually seeing the reason. The reasons are often made clear in your error logs. This is how to read them.

Back in the early 1900s (when horses, trains, and your feet were the primary mode of travel), it required the terminal to really deal with your error logs. You'd ask for help on a forum and they'd want you to run something like:

[code]grep -i "Feb 10" /var/log/*.log | sort | uniq -c | sort -n[/code]

It worked and it worked well, especially if you knew what you were looking for. If you weren't, then you'd be scrolling through tons of text in the terminal with few visual cues or no easy way to sort through the data.

Well, enter KSystemLog. KSystemLog's man page describes it as thus:

Description: system log viewer
KSystemLog show all logs of your system, grouped by General (Default system
log, Authentication, Kernel, X.org…), and optional Services (Apache, Cups,
etc, …). It includes many features to read nicely your log files:
* Colorize log lines depending on their severities
* Tabbed view to allow displaying several logs at the same time
* Auto display new lines logged
* Detailed information for each log lines
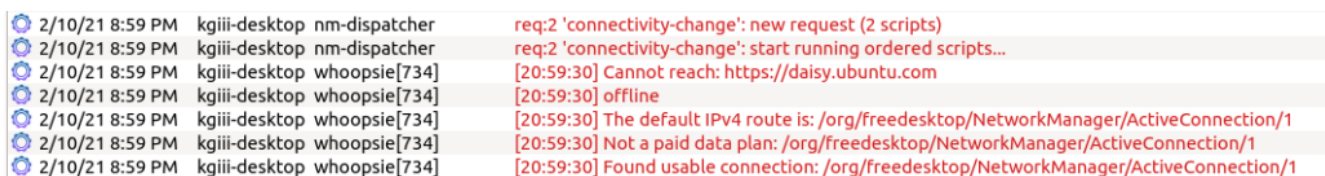
And it looks like this:
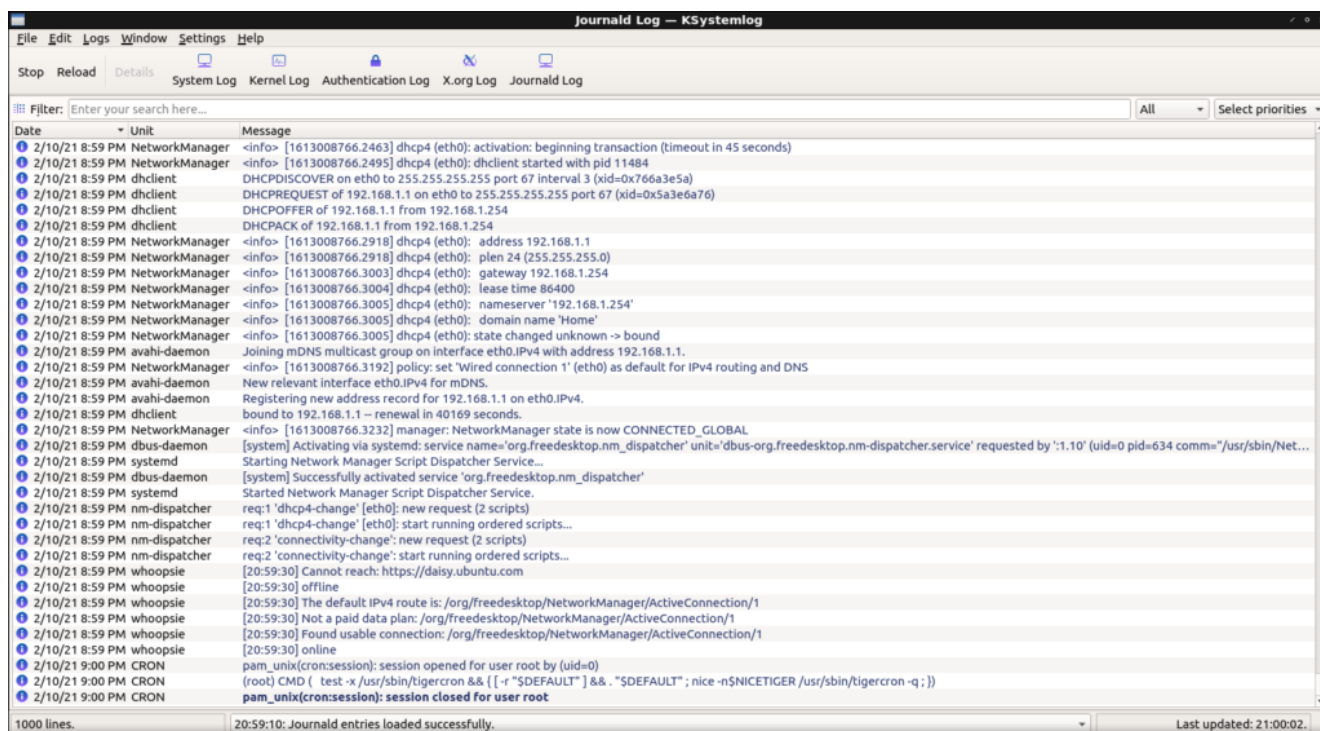
KSystemlog UI — not pictured, fancy colors

As you can see from the image, this is a handy GUI method to view your various system logs. If you look at the image above, you'll see that one of the lines is a darker blue than the previous lines. This is because it was a new log entry, an event that happened after I'd opened the application.

So, in other words, you can open KSystemLog and then open an application that's giving you trouble and see what errors are thrown. You can also examine the entire list of errors and events.

Not only that, but the events in the logs are color-coded. This provides easy visual cues as the events range in color from a light gray (normal) to a bright red for emergency-level events. You can also apply filters and search for specific events.

Note the color change for errors.

KSystemLog is a KDE application but pulls in very few dependencies. It loads rapidly and will pick up all installed log files by default. In my case, it finds these:
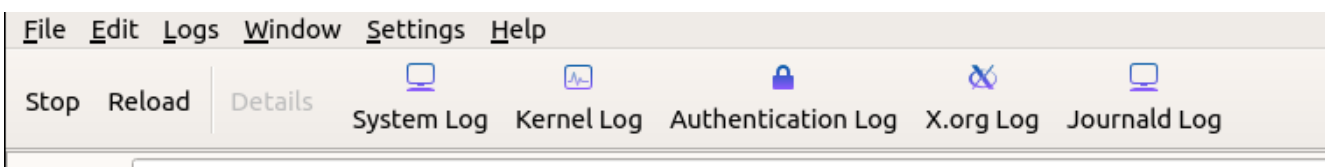
Currently available logs on this particular system.

Chances are pretty good that it is in your default repositories. If you're using a Debian derivative then you can install it by opening the terminal and entering:

[code]sudo apt install ksystemlog -y[/code]

Anyhow, there you have it. Adjust the above command for your distro's package manager (or go dig it out if you're manually installing packages). You can take the information from the logged errors and use them as search terms to help.

It's absolutely amazing how many errors can be resolved by just taking the exact error message and tossing it verbatim into a search engine of your choice. I've used this method to troubleshoot so many times that I think it's an asset we should all have in our toolbox.

As always, go ahead and subscribe to get notifications when new articles are published. If you want, you can go ahead and register and start helping. If you don't want to maintain your own site and want to write articles, that can be arranged. Thanks for reading!