# USN-4737-1: Bind vulnerability

It was discovered that Bind incorrectly handled GSSAPI security policy
negotiation. A remote attacker could use this issue to cause Bind to crash,
resulting in a denial of service, or possibly execute arbitrary code. In
the default installation, attackers would be isolated by the Bind AppArmor
profile.

---

# USN-4734-2: wpa_supplicant and hostapd vulnerabilities

USN-4734-1 fixed several vulnerabilities in wpa_supplicant. This
update provides the corresponding update for Ubuntu 14.04 ESM.
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)

# USN-4736-1: Thunderbird vulnerabilities

Multiple security issues were discovered in Thunderbird. If a user were
tricked into opening a specially crafted website in a browsing context,
an attacker could potentially exploit these to cause a denial of service,
obtain sensitive information, or execute arbitrary code. (CVE-2020-26976,
CVE-2021-23953, CVE-2021-23954, CVE-2021-23960, CVE-2021-23964)
It was discovered that responses received during the plaintext phase of
the STARTTLS connection setup were subsequently evaluated during the
encrypted session. A person in the middle could potentially exploit this
to perform a response injection attack. (CVE-2020-15685)

# 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?