

Forum:[Hack Forums](#)

Thread: [Linux CUPS Vulnerability Allow Remote DoS and Admin Authentication Bypass](#)

JoseMar - September 15, 2025, 2:41 am

Linux CUPS Vulnerability Allow
Remote DoS and Admin Authentication Bypass

Two CUPS bugs just popped

Look, I try not to be the guy yelling about printers. But this one actually matters. Two CUPS bugs just popped up and they are exactly the kind of boring, petty little failures that turn into network drama fast.

If you run Linux anywhere that shares a network with other things, yes, that includes your office, the lab, that classroom PC, pay attention. I'll explain like I'm muttering into the ticket system while making coffee.

Remote DoS: The Annoying One

CVE-2025-58364. Ugly name, simple result: crash. The lib cups code path for printer attribute parsing has a nasty null deref scenario. Throw in a malformed printer attribute response and the `ipp_read_io()` function trips over itself. Loop tries to read a string that isn't there. Boom, cups dies, prints stop, panic ensues.

Now the caveat: you need adjacent network access. So it is not some random Internet spray. But that does not help much in a lot of places. Shared Wi Fi in offices, labs, even a hotel network, those are flat enough that an attacker can get next to the target. And cups-browsed? If that service is on, it'll happily listen for announcements and make discovery easy. It's the kind of thing that lives on old boxes nobody logs into anymore. You know the ones. The small Debian VM running something important enough to be annoying if it stops.

Also, no patch at the time of writing. So for now it's mitigation and hoping someone pushes a fix soon.

Auth Bypass: The Scary One

CVE-2025-58060. This one made me sit up. AuthType Negotiate, Kerberos, LDAP, you set those up because you want real security. Except the scheduler/auth.c logic in `cupsdAuthorize()` apparently skips password validation if an incoming request contains a Basic header. So an attacker can send Authorization: Basic with basically any password and get in.

Let that sink in. You harden your printing infra with enterprise auth, and some edge-case logic says, yeah, Basic is fine, go ahead. Poof: admin-level access with a header and a base64 string. You can tweak configs, drain queues, maybe run whatever limited admin actions CUPS exposes. It is not full root on the box, sure, but it's the kind of foothold that lets you be extremely annoying and,

depending on the environment, quietly dangerous.

I keep imagining some intern or bored researcher testing this and suddenly being able to delete months of print jobs. Hilarious in theory, terrible in practice.

What To Do (Until They Fix It)

Short checklist, because nobody needs a dissertation right now: Block port 631 at the network edge unless you absolutely need it. Seriously, firewall it.

Disable cups-browsed unless you rely on automatic discovery. If you don't know why it's on, turn it off.

If you use Negotiate/Kerberos/LDAP for CUPS, consider reverting to Basic with a strong password for the moment. I know, I know, it feels wrong. But the bypass makes the fancy auth worse than the simple one until there's a patch.

Audit weird, old print servers, the dusty VM in a corner is a likely candidate. Update, isolate, or retire it.

None of those are glamorous. They are annoying and they work. If you manage things for a shop, automate the checks. If you're a hobbyist with one or two machines, check `systemctl status cups` and `ss -ltnp | grep 631` and be done.

What bugs me most is the repeat pattern.

The tiny, under-loved subsystems keep biting us. Printers are the perfect toy for low-effort but effective attacks: they talk on networks, they often run with elevated capabilities, they are rarely monitored. Add one sloppy validation check and a weird auth code path, and suddenly you have two completely different attack surfaces on the same service.

I don't want to overdramatize. This isn't a complete takeover of everything. But it is exactly the sort of thing that turns a boring Tuesday into a very long one for whoever's on call. If you want to be smug about security, great. If you want to be realistic, check your CUPS exposure now.

Anyone here already pulled the plug on cups-browsed? Or rolled back auth configs? Tell me what you did and whether it broke anything else. I'll take messy real-world reports over polished advisories any day.