Concierge Digital Solutions

CDS Tech Tips

Monthly Security & Technology Insights

Hello from CDS,

August brings a busy month for security updates, and there's one important vulnerability you need to know about. If you use VPN services or remote access on your Windows computers, there's a critical patch waiting for you. The good news? Taking action is simple, and we'll walk you through it. Plus, we've got three quick tasks that'll make your systems more secure right now.

— Ron Willitzer

⚠ CRITICAL ALERT

Important: A Critical Security Update Your Windows Systems Need

Here's the straightforward version: A vulnerability has been discovered in Windows that lets attackers access your computer remotely. It's already being actively exploited by bad actors. If your organization uses VPN services or remote access, this affects you. The good news? Microsoft has released a patch, and installing it is the solution.

What to watch for:

- Unexpected crashes or restarts on your VPN servers or remote access computers
- Strange behavior from your VPN connections
- Anyone warning you about unusual remote access attempts

How to stay safe: Install the August Windows security update as soon as possible. We know updates can be disruptive, but this one is worth the restart. If VPN is not something you use, you're still protected by the patch. If you have questions about whether this affects your setup or need help applying the patch, just give us a call. We can walk you through it or handle it remotely.

🔒 SECURITY UPDATES

Your August Update Checklist: Windows and Mac

August's security updates include fixes for several important Windows and Mac vulnerabilities. Think of these patches as regular maintenance—they keep your systems running safely and securely. Here's what you need to do:

Windows computers and servers: These updates matter, and getting them installed correctly (especially across multiple machines) is exactly what we handle for our managed clients. If you haven't heard from us about this yet, give us a call and we'll make sure your systems are covered.

Mac users: Same idea applies — staying current on updates matters, and we keep an eye on this for our managed Mac clients so you don't have to think about it. Mac systems tend to have fewer security

headaches than Windows, but that doesn't mean we should skip updates. One thing to note: Mac users often face phishing and social engineering attempts more than malware, so your awareness is your best defense. Stay skeptical of unsolicited emails and links.

The real story: Windows systems encounter more malware than Mac systems (six times more, according to recent reports), but that's partly because there are more Windows computers in the world. Regardless of your operating system, keeping your software updated is one of the single best things you can do.

💡 QUICK TIPS

3 Things to Do This Month

1. **Update Your Devices** Make sure your Windows and Mac systems are current on updates this week. If you're a managed client, we've likely already got this covered — but a quick check never hurts.

2. **Check Your Remote Access** If you use VPN or remote access, now's a good time to review who can access what. Make sure only the people who need remote access actually have it. If you're not sure, reach out and we can review it together.

3. **Be Skeptical of Emails** This month and every month: if an email looks even slightly suspicious (unexpected sender, urgent language, weird links), don't click it. Forward it to us or ask your IT person. A little caution prevents a lot of headaches.

Uncertain about your updates or want a second opinion? We're here to help.

📞 832-378-8393

Schedule Security Review

Concierge Digital Solutions

Keeping your technology running smoothly since 2017

832-378-8393 | ron@cdsolutions.net

www.cdsolutions.net