

SECURITY ALERT · 22 OCTOBER 2026

PHP2Shell: The One-Hour Check

For businesses whose phone system runs on their own server. Five questions for your IT person today, and the technical steps behind them.

Two critical flaws in PHP, CVE-2026-109618 and CVE-2026-109619, were fixed on 21 October 2026 and attack traffic followed within hours. One web request, no password. PHP runs the admin screens of many self-hosted phone systems, and those screens are often on the open internet.

■ Does it apply to you?

Your setup	What to do
FreePBX, PBXact, Issabel, FusionPBX	Check today
VoIP billing such as ASTPP	Check today
Self-hosted 3CX	Check what else shares the server and network
An old system nobody touches	Check today, assume the worst
Cloud, provider runs it	Ask the provider what they patched

■ What is on that server

- Call recordings and voicemail
- Call records: your customer list
- The login used to make calls on your account
- A foothold inside your office network

■ Why it is urgent

- Rated 9.2 out of 10
- No password needed
- Probing seen before the fix was public
- Updating the phone software alone does not fix it

■ Five questions for your IT person, today

- 1 Which PHP version, and is it a fixed release? 8.5.12, 8.4.27, 8.3.36, 8.2.35 or a patched package.
- 2 Has everything been restarted since? Old code stays in memory until it is.
- 3 Can the admin screen be reached from the internet? It should be VPN or approved addresses only.
- 4 Have the logs and call records been checked since 20 October?
- 5 What spend limits and international barring are in place? They cap the damage.

■ For your IT person

Step	Detail
Patch	Fixed release or distro package. Check the web SAPI, not just php -v. 8.1 and older: source backports only.
Restart	Every PHP-FPM pool and Apache.
Interim	session.upload_progress.enabled = 0; memory_limit = -1 plus a cgroup limit; fatal_error_backtraces = 0 on 8.5. php.ini or pool config, then restart. Not a fix.
Edge	Admin GUI behind VPN or allow list. Block or cap multipart requests.
Hunt	PHP_SESSION_UPLOAD_PROGRESS multipart POSTs, ----p2s boundaries, memory exhausted bursts, large PHPSESSID, odd child processes, new files or cron jobs, unusual CDRs.
Contain	Rotate SIP, admin and API credentials if it was public and unpatched.

How it works, in one paragraph

An out of memory bailout can leave request data half built for cleanup to trust (CVE-2026-109618), and request state can outlive its memory into the next request on the same worker (CVE-2026-109619). Session upload progress processes multipart bodies before any application code runs, so any page that accepts a POST is a way in. Apache mod_php is the highest risk.

If the answer is "not sure"

Take the admin screen off the internet today. If the server cannot be updated quickly, take it offline and divert your main number to mobiles until it is. If there are signs of a break in, rebuild, do not just patch, and report it through ReportCyber.

A note for 3CX customers

3CX runs its own web server and database and is not on the NCSC-NL list, so PHP2Shell is not a 3CX flaw on current evidence. Other PHP software on the same server or network, or shared passwords, can still expose it.

VOCPhone

No phone server on your side to patch. We own and operate our network in Australia, and vocphone.com was on PHP 8.5.12 when checked on 22 October. \$0 setup, \$0 porting. 1300 663 222.