

SECURITY ALERT · 22 OCTOBER 2026

PHP2Shell and Self-Hosted Phone Systems

Two critical PHP flaws, CVE-2026-109618 and CVE-2026-109619, fixed on 21 October and probed within hours. What they are, which PBX platforms run PHP, and the steps to take today.

PHP2Shell is a pair of bugs in the PHP runtime itself, not in any one application. Both are rated 9.2 (CVSS v4), both can be reached by a single request from someone who has not logged in, and exploit shaped traffic was seen before the fix was even public. Any phone system managed through a PHP admin panel is in scope.

Fixed releases

Branch	Fixed in	Note
8.5	8.5.12	Update now
8.4	8.4.27	Update now
8.3	8.3.36	Update now
8.2	8.2.35	Update now
8.1, 8.0, 7.4	No php.net release	Source backport or vendor package
7.3 and older	None	Upgrade or take offline

How it works

- **CVE-2026-109618:** an out of memory bailout (a longjmp) leaves request data half built, and cleanup trusts it.
- **CVE-2026-109619:** request state survives after its memory is freed, and the next request on the same worker uses it.
- **No login:** session upload progress processes multipart bodies before any application code runs.
- **Highest risk:** Apache mod_php, PHP-FPM, php-cgi, FrankenPHP and LiteSpeed are also affected.

Why a PBX is a prize

- The FreePBX web server runs as the asterisk user.
- Call recordings and voicemail on the same disk.
- Call records: a map of your customers.
- SIP trunk credentials, and so toll fraud.
- A quiet foothold on the office network.

Phone platforms (NCSC-NL tracker, 22 Oct)

Platform	PHP	Status
FreePBX 17 / PBXact 17	8.2	Investigation
Issabel 5	7.4	Investigation
FusionPBX	FPM, per install	Vulnerable on affected PHP
ASTPP v7 billing	8.2	Vulnerable
3CX	No public sign of PHP	Not listed

■ What to do today

- 1 **Find every PHP serving web requests** on the PBX and anything sharing its host or network. Check the web SAPI, not just php -v.
- 2 **Update** to a fixed release or your distribution's patched package.
- 3 **Restart every worker:** all PHP-FPM pools and Apache.
- 4 **Interim, if you cannot patch:** session.upload_progress.enabled = 0, memory_limit = -1 with a cgroup limit instead, fatal_error_backtraces = 0 on 8.5. Set in php.ini or pool config, then restart. Not a fix.
- 5 **Take the admin panel off the internet:** VPN or allow list only, and keep it that way.
- 6 **Limit requests at the edge:** block multipart where there are no uploads; cap size, parts and fields where there are.
- 7 **Cannot do any of that?** Take it offline and send calls to mobiles.
- 8 **Was it public and unpatched?** Rotate SIP and admin credentials, set carrier spend limits, bar international calls you do not need.

■ Signs of an attempt

- ☐ Multipart POSTs with PHP_SESSION_UPLOAD_PROGRESS, boundaries starting ----p2s
- ☐ Bursts of "Allowed memory size exhausted" and worker crashes
- ☐ Oversized PHPSESSID values in Set-Cookie
- ☐ PHP or asterisk processes spawning shells, curl or wget
- ☐ New PHP files, cron entries or SSH keys
- ☐ Overnight or weekend calls to international or premium numbers

Found something? Do not just patch

Patching stops the next attacker, not the one already inside. Isolate the box, keep the logs, rebuild from known good media with fresh credentials, report through ReportCyber, and assess the Notifiable Data Breaches scheme.

Where 3CX fits

3CX runs its own Nginx and PostgreSQL and is not on the tracker, so PHP2Shell is not a 3CX bug on current evidence. A 3CX box that shares a server, network or admin passwords with PHP apps is still exposed through them.

The Uniden Voice side

There is no PBX server for you to patch: the platform is ours to run in Australia. unidenvoice.com was on PHP 8.5.12 when checked on 22 October. Free setup and porting. Book a demo on 1300 881 662.