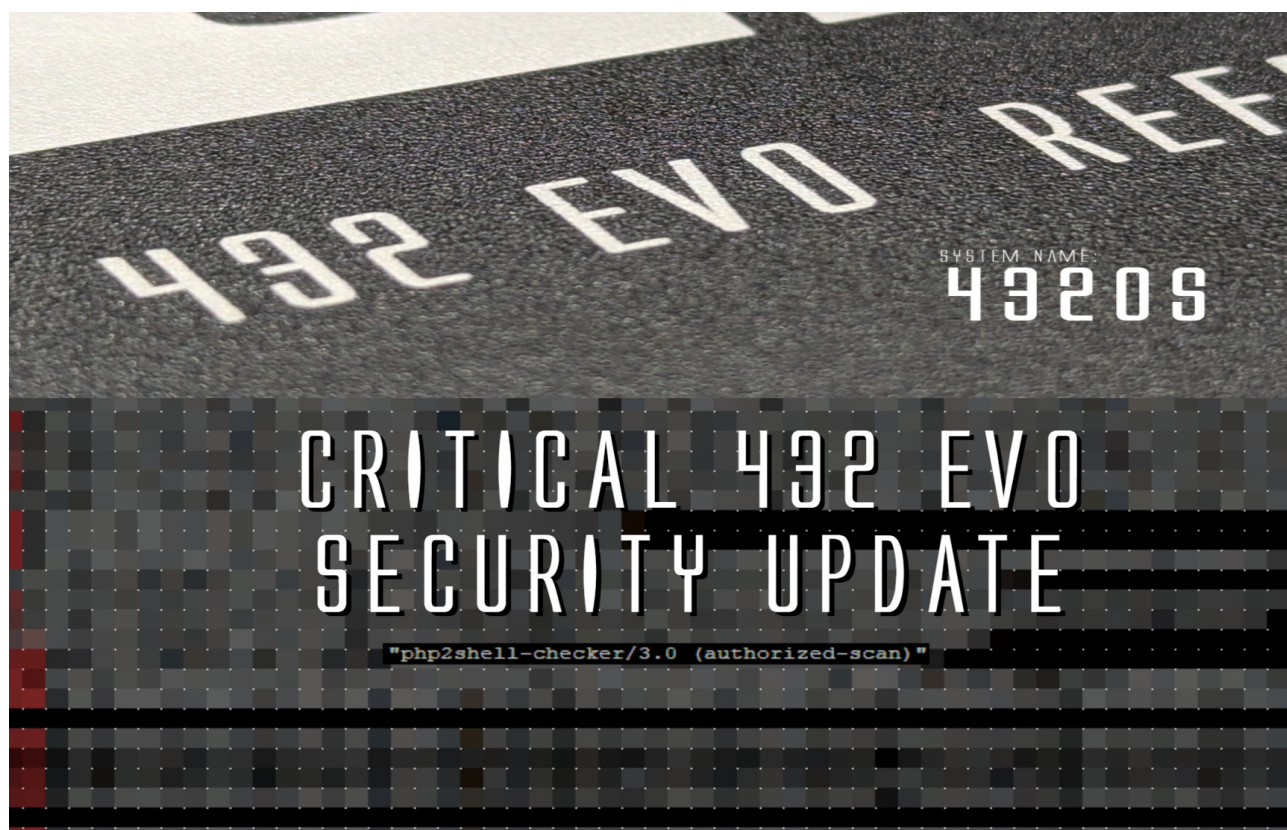




432 EVO REFERENCE MUSIC SERVER



Date: 22/10/2026

CRITICAL 432 EVO
SECURITY UPDATE

The latest version can be found here:

<https://432evo.be/4320S-php2shell-protecton.pdf>

Executive Summary: the PHP2Shell Threat

On October 21, 2026, a critical set of high-impact vulnerabilities known as PHP2Shell (CVE-2026-109618 and CVE-2026-109619) hit the internet, affecting roughly 70% of internet-facing sites running PHP.

These vulnerabilities permit remote command execution (RCE), allowing bad actors to run code directly on affected servers without login credentials. While cloud webserver were forced offline globally, 432 EVO's web application firewall successfully blocked initial attempts.

However, to ensure absolute safety, an immediate update is also required for all active 432OS based music servers, since the 432 EVO GUI currently depends on PHP. 432 EVO servers based on the old OS no longer receive updates, and are required to update to 432OS to receive any updates including security patching.

More info:

<https://en.wikipedia.org/wiki/PHP2Shell>

<https://432evo.be/index.php/2025/06/16/os-support-update/>

How did 432 EVO respond?

1. How 432 EVO Secured Its Public Sites

432 EVO took decisive, immediate action to protect its public web presence against PHP2Shell:

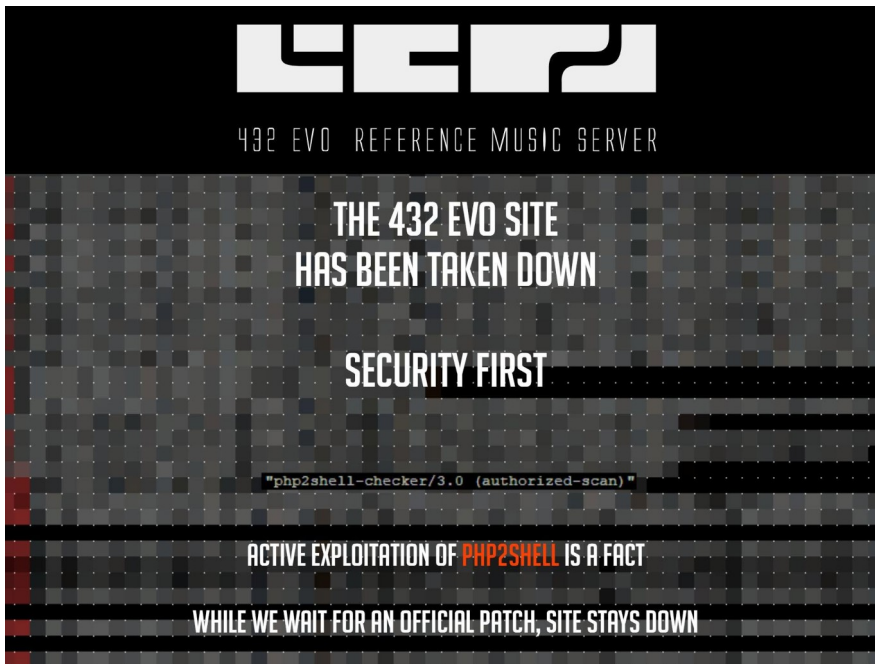
1. Retiring the Legacy v1 Site:

On October 21, 2026, 432 EVO permanently disabled PHP and took down the old CMS running on v1.432evo.be to eliminate legacy vulnerabilities. Technical articles hosted there are being safely migrated to a different platform.

2. Active Web Application Firewall (WAF) Defense:

The primary public sites (432evo.be and my.432evo.be) were already hardened with custom WAF rules since years. These rules successfully blocked the actual incoming php2shell-checker/3.0 attacks logged against 432 EVO's infrastructure. PHP2Shell was also [detected by Cloudflare](#): Cloudflare CEO Matthew Prince said the company's network had seen millions of attempts to exploit the PHP2Shell vulnerabilities, including thousands during the 10 hours before they were publicly announced.

3. Minimal Downtime & Rapid Restoration:



On October 21th at around 15:00, mainstream news channels and tech sites were announcing several sites being taken down as a precaution. We took down the main 432 EVO website, to do audits, while posting a message on social media. Benelux tech site tweakers.net did something very similar.

Following a swift audit of WAF rules, configurations, and server logs, the currently secure websites were quickly brought back online.

2. How is 432 EVO securing it's music servers in the field?

432 EVO Music Servers use PHP as the scripting language for the current GUI, and are also affected by the same PHP bugs. Since the 432 EVO music servers are not directly internet facing, contrary to a datacenter/cloud based webserver, the security risk is much lower, but still not zero.

Why 432 EVO Runs on AlmaLinux (And Why Competitors Fall Short)

Many music server competitors base their 2026 hardware/software on outdated platforms like Debian 10 or Debian 11, which have already reached End-of-Life (EOL) and no longer receive security patches. The same applies to the old vortexbox os. Patching an ancient OS forever is simply not possible security wise.

1. Debian 10-based servers (LMS-based brands): EOL on June 30, 2024
2. Debian 11-based servers (MPD-based brands): EOL on August 31, 2026
3. 432 EVO Old OS (Vortexbox): EOL in December 2025 → **upgrade to 432OS now**

Users of the old "vortexbox" end of life OS will not receive any updates which fix these PHP issues:

<https://432evo.be/index.php/2025/06/16/os-support-update/>

The 432 EVO 432OS Advantage: Enterprise-Grade Lifecycle



432OS is based on AlmaLinux, benefiting from a robust 10-year enterprise security patching lifecycle.

Current 432OS builds receive **security updates backed through May 31, 2032**, with plans already underway to **extend this support to May 31, 2035**.

The currently used version is AlmaLinux 9.8, where the minor version (the .8) is updated and retested every 6 months. Your current version is also visible in the web gui.

The "EVO" in 432 EVO: a Future-Proof Hardware Design

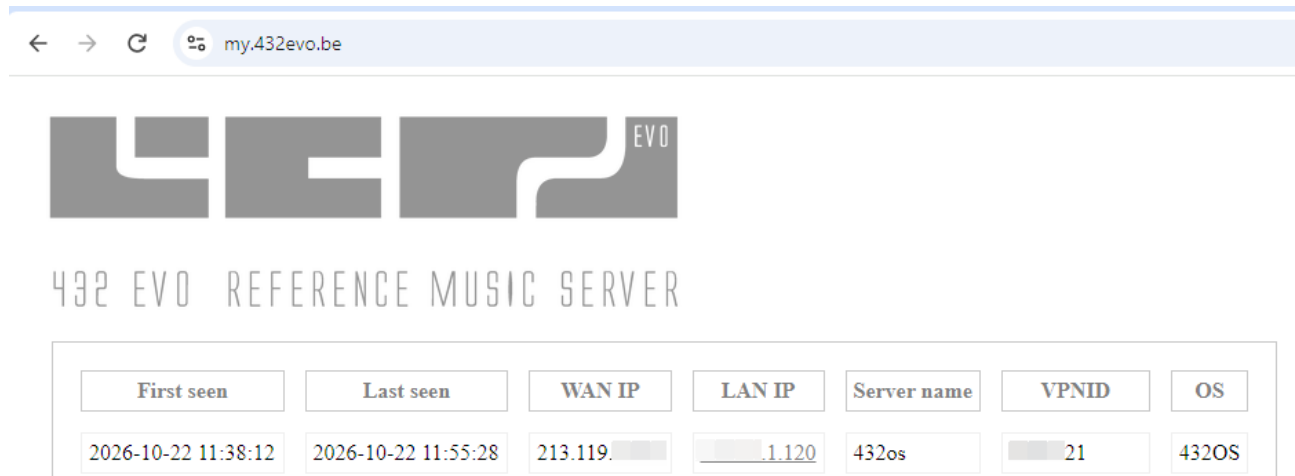
Unlike competitors using milled chassis with connector cutouts locked into specific, obsolete motherboards (such as the outdated N4200) currently in the field, 432 EVO has offered a complete upgrade path for internal computer and storage components across every build since 2013.

Step-by-Step Update Guide For 432OS Users

If you are running 432OS, follow these steps to secure your music server server against PHP2Shell:

Step 1: surf to my.432evo.be

From a computer connected to the same local network as your music server, navigate to my.432evo.be, and click on the LAN IP



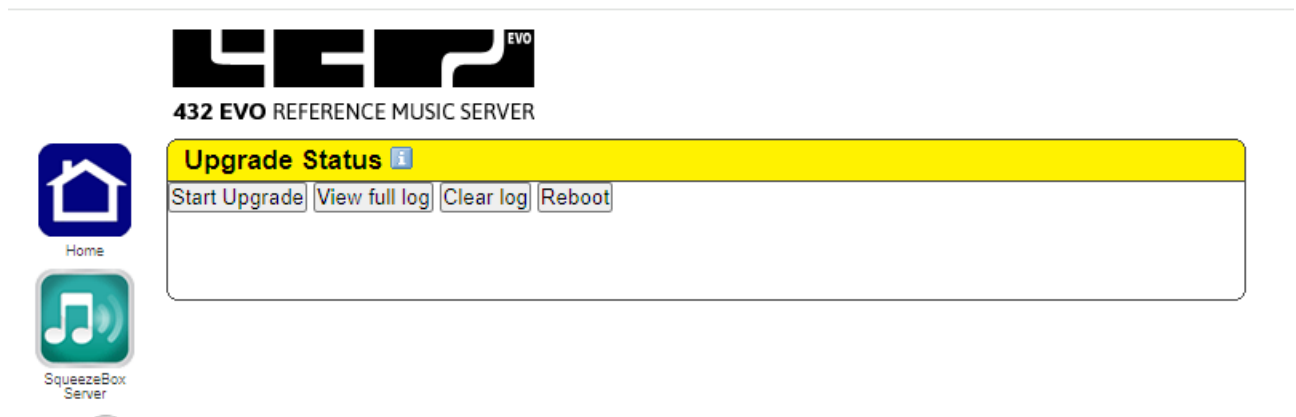
Step 2:

In the 432 EVO Web Gui, click on “432 EVO Upgrade”, the icon in the bottom left column:



Step 3:

Click on Start Upgrade:



The installer will update the vortexbox package first. It may throw a non-critical Python/tempfile exception or stop due to package conflicts during the first pass—this is normal:



Step 4: Handling Potential Installer Error Cases

Check if there were any errors in step 3 or in step 4:

Case 1: "Cannot create temporary file"

In case the error is "cannot create temporary file"

```
Traceback (most recent call last):
  File "/usr/lib64/python3.9/tempfile.py", line 461, in __del__
    self.close()
  File "/usr/lib64/python3.9/tempfile.py", line 457, in close
    unlink(self.name)
FileNotFoundError: [Errno 2] No such file or directory: '/tmp/tmp1shcgl6m'

Upgraded:
vortexbox-2.3-20261022rhe19.i686

Complete!
Cannot create temporary file - mkstemp '/tmp/librepo-tmp-SCki9C': No such file or directory
10/22/2026 12:41:51 - Error: yum update failed. Check error messages and try to fix problems.
```

Simply click **Start Upgrade** a second time to bypass temporary file glitches.

Case 2: "Duplicate packages" conflict (PHP-common / Nginx)

If the log displays a conflict regarding php-common versions, just run Start Upgrade again.

```
Error:
Problem: package php-fpm-8.0.30-8.el9_8.x86_64 from @System requires php-common(x86-64) = 8.0.30-8.el9_8, but none of the
providers can be installed
- cannot install both php-common-8.0.30-8.el9_8.alma.1.x86_64 from appstream and php-common-8.0.30-8.el9_8.x86_64 from @System
- cannot install both php-common-8.0.30-8.el9_8.x86_64 from appstream and php-common-8.0.30-8.el9_8.alma.1.x86_64 from appstream
- cannot install the best update candidate for package php-common-8.0.30-8.el9_8.x86_64
- problem with installed package php-fpm-8.0.30-8.el9_8.x86_64
(tr try to add '--allowerase' to command line to replace conflicting packages or '--nobest' to use not only best candidate packages)
10/22/2026 12:56:34 - Error: yum update failed. Check error messages and try to fix problems.
```

The updated installer will detect the conflict, display a "Manually fixing problems with packages!" prompt, and automatically apply the necessary alma.1 patches containing the official PHP2Shell fix.

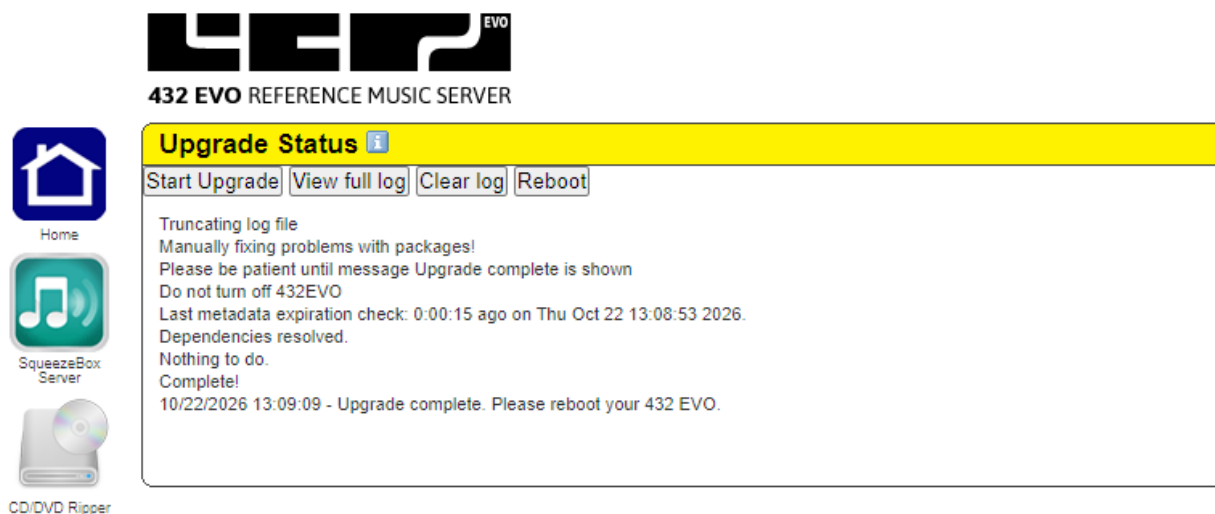
```
10/22/2026 13:08:07 - Starting upgrade. (This can take a long time...)

90 files removed
432OS 70 kB/s | 12 kB 00:00
Dependencies resolved.
Nothing to do.
Complete!
Manually fixing problems with packages!
Please be patient until message Upgrade complete is shown
Do not turn off 432EVO
```

Note: Do not turn off your 432 EVO while this process finishes!

Step 5: Completion & Reboot

Once the upgrade script finishes processing dependencies, you will see the message "Nothing to do" followed by "Upgrade complete. Please reboot your 432 EVO"



Click Reboot to finalize your system protection

What happens under the hood?

PHP on 432OS is currently based on the php:8.0 stream, and after updating, internally your server will be on 8.0.30-8.el9_8.alma.1 versions instead of 8.0.30-8.el9_8, so after the update you will at least have:

```
2026-10-22T13:09:06+0200 DEBUG Upgraded: php-cli-8.0.30-8.el9_8.alma.1.x86_64
2026-10-22T13:09:06+0200 DEBUG Upgraded: php-common-8.0.30-8.el9_8.alma.1.x86_64
2026-10-22T13:09:06+0200 DEBUG Upgraded: php-fpm-8.0.30-8.el9_8.alma.1.x86_64
2026-10-22T13:09:06+0200 DEBUG Upgraded: php-intl-8.0.30-8.el9_8.alma.1.x86_64
2026-10-22T13:09:06+0200 DEBUG Upgraded: php-mbstring-8.0.30-8.el9_8.alma.1.x86_64
2026-10-22T13:09:06+0200 DEBUG Upgraded: php-process-8.0.30-8.el9_8.alma.1.x86_64
...
```

which are the patched versions:

<https://almalinux.org/blog/2026-10-21-php2shell-cve-2026-109618-cve-2026-109619/>

In the future we intend to make the updater more user friendly and handle the exceptions automatically.

However, since we believe in a Security First principle, having patching against this massive PHP vulnerability, currently has the highest priority.

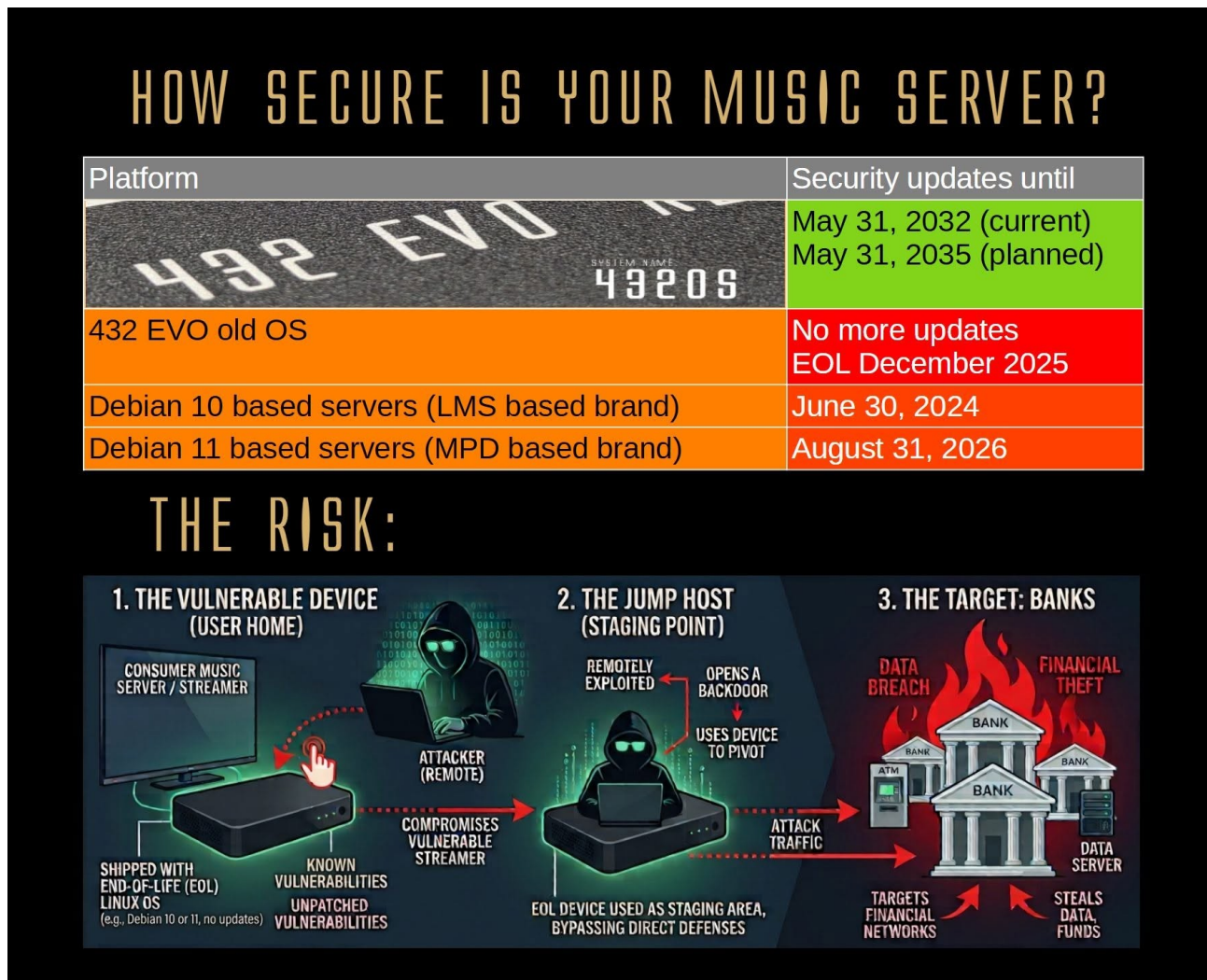
What happens if I do not update 432OS or keep using the old OS?

While music servers reside behind home routers (NAT) and are not directly exposed to the open internet, local risks remain severe if left unpatched:

The Vulnerable Device:

An unpatched consumer music server running end-of-life Linux, or currently supported Linux but without security updates, will contain active vulnerabilities!

The Jump Host / Staging Point:



If a network is misconfigured (e.g., placed in a DMZ or ports forwarded improperly), or attacked from within your home LAN from another compromised device, attackers can remotely exploit the device, open a backdoor, and pivot into the home network.

Real-world security incidents have shown hackers installing proxies on unpatched servers to route illegal traffic (such as cyberattacks against banking networks), leaving the server owner legally liable

The Target: Unpatched RCE vectors like PHP2Shell provide the exact backdoor entry points that compromise home infrastructure. Imagine at least 70% of the internet becoming a jumphost for hackers. This is why the internet was literally on fire on October 21st 2026, and 432 EVO took

immediate action to protect both it's website, and it's customer's music servers.

Protect your investment and secure your network, and ensure long-term peace of mind by updating your 4320S operating system today. If you are still on the outdated vortexbox based OS, upgrade now!

If you encounter any persistent errors during the procedure in this guide, contact 432 EVO support directly mentioning your server's **VPNID**.

Some links with more details for technical people:

<https://en.wikipedia.org/wiki/PHP2Shell>

<https://almalinux.org/blog/2026-10-21-php2shell-cve-2026-109618-cve-2026-109619/>