

Закреть уязвимость PHP2Shell: порядок работ и проверки

CVE-2026-109618 и CVE-2026-109619 · исправления PHP от 21 октября 2026 года · обновление CMS уязвимость не закрывает

8.5.12

ветка 8.5 и новее

8.4.27

ветка 8.4 и новее

8.3.36

ветка 8.3 и новее

8.2.35

ветка 8.2, поддержка до 31.12.2026

1. Инвентаризация

- ☐ Список всех сайтов, поддоменов и серверов компании, где работает PHP, включая старые лендинги и обработчики форм.
- ☐ Версия PHP, которая обслуживает каждый сайт: phpinfo, раздел «Сервер» в CMS или php-fpm -v. Консольный php -v не в счёт.
- ☐ Способ запуска: PHP-FPM, Apache с mod_php, CGI, LiteSpeed, FrankenPHP. Самый высокий риск у mod_php.
- ☐ Если пакет из дистрибутива: есть ли CVE-2026-109618 и CVE-2026-109619 в журнале изменений пакета (номер версии может не меняться).

2. Резервная копия до изменений

- ☐ Файлы сайта, база данных и конфигурация сервера, лучше снимок виртуальной машины.
- ☐ Копия проверена: открывается, база разворачивается.
- ☐ Копия лежит отдельно от сервера сайта.

3. Обновление

- ☐ Ветки 8.2 до 8.5: исправленный выпуск своей ветки (8.2.35, 8.3.36, 8.4.27, 8.5.12) или пакет дистрибутива с исправлением.
- ☐ Ветки 7.4, 8.0, 8.1: сборка хостинга или дистрибутива с исправлением, переход на 8.3 или 8.4 поставлен в план.
- ☐ Ветка 7.3 и старше: исправления нет, сайт закрыт от интернета до перехода.
- ☐ Перезапущены PHP-FPM или Apache. Перезапуска одного nginx недостаточно.
- ☐ Docker: образ пересобран на свежей базе, контейнер пересоздан с сохранением томов.
- ☐ Обновлено все сайты, пулы и все серверы, если их несколько.

4. Проверка после обновления

- ☐ Исправленную сборку видит сам сайт (phpinfo или раздел «Сервер» в CMS).
- ☐ Работают вход, формы, загрузка файлов, корзина и оплата, обмен с 1С и CRM, почта с сайта.
- ☐ На 8.4.27 и 8.5.12 проверены выгрузки и импорт через XML: в этих выпусках найдена ошибка SimpleXML (задача 24488), исправление войдёт в следующий выпуск.
- ☐ Журналы PHP и веб-сервера без новых фатальных ошибок за первые сутки.

5. Признаки взлома, смотреть с 17 октября 2026

- ☐ Запросы с полем PHP_SESSION_UPLOAD_PROGRESS и странные multipart/form-data с ошибками 500 после них.
- ☐ Ошибки памяти «in Unknown on line 0» в журнале PHP.
- ☐ Процессы веб-сервера или PHP запускают sh, bash, curl, wget.
- ☐ Новые или изменённые PHP-файлы, особенно в папках загрузок, новые задания cron, незнакомые администраторы.
- ☐ Нашли следы: сохранить копию сервера и журналов, отключить сайт, сменить все пароли и ключи, восстановить из чистой копии до 17 октября.

6. Если обновиться сегодня нельзя

- ☐ session.upload_progress.enabled = Off в php.ini или пуле, затем перезапуск PHP. Закрывает только часть путей атаки.
- ☐ Лимиты на размер и число частей multipart-запросов на веб-сервере.
- ☐ Правила WAF у хостинга или облачного WAF.
- ☐ Сайт или админка закрыты от интернета до обновления.

Нужна помощь? Optimism бесплатно проверит, какая версия PHP стоит на вашем сайте и закрыта ли уязвимость. Срочное обновление PHP от 20 000 Р, помощь при взломе, техническая поддержка от 23 000 Р в месяц. +7 (495) 118-20-98 · go@optimism.ru · optimism.ru/services/sitemaking/tekhnicheskaya-podderzhka/