

НКЦКИ

НАЦИОНАЛЬНЫЙ КООРДИНАЦИОННЫЙ ЦЕНТР
ПО КОМПЬЮТЕРНЫМ ИНЦИДЕНТАМ

Веб-сайт: cert.gov.ru

E-mail: threats@cert.gov.ru

Эксплуатация критических уязвимостей в PHP (CVE-2026-109618, CVE-2026-109619)

ALRT-20261022.1 | 22 октября 2026 г.

Уровень угрозы: КРИТИЧЕСКИЙ

TLP: WHITE



	20 октября 2026 г. команда разработчиков PHP опубликовала предварительное уведомление о двух критических уязвимостях, получивших общее название PHP2Shell и идентификаторы CVE-2026-109618 и CVE-2026-109619. Обе уязвимости позволяют неаутентифицированному удалённому злоумышленнику выполнить произвольный код на уязвимом сервере. Уязвимости затрагивают все версии PHP, начиная с 5.4.0, и присутствуют в самом ядре языка. Официальные исправления выпущены 21 октября 2026 г. для версий PHP 8.5.12, 8.4.27, 8.3.36 и 8.2.35; для устаревших версий 7.4, 8.0, 8.1 также подготовлены патчи. CVE-2026-109618, повреждение памяти при обработке (Out-of-Memory, OOM). При выделении памяти PHP может аварийно прервать обработку запроса, оставив внутренние данные частично инициализированными. Специально сформированные multipart-запросы (используемые для форм и загрузки файлов) способны исчерпать память даже при соблюдении настроенных ограничений, что приводит к использованию повреждённых данных и последующему выполнению кода. Наиболее высокому риску подвержен Apache mod_php, поскольку эксплуатация может быть успешной до запуска кода приложения. CVE-2026-109619, использование памяти после освобождения (use-after-free). PHP повторно использует рабочий процесс для обработки нескольких HTTP-запросов. Внутреннее состояние, указывающее на память, освобождённую при завершении предыдущего запроса, может сохраняться и быть доступным для следующего запроса до момента его нормальной инициализации. Это позволяет удалённому злоумышленнику получить контроль над потоком выполнения и выполнить произвольный код.
Рекомендуемые меры по нейтрализации угроз	1. Обновить PHP до версий: 8.5.12, 8.4.27, 8.3.36 или 8.2.35. После обновления перезапустить PHP-FPM, Apache или соответствующий веб-сервер, чтобы загрузился исправленный бинарный файл. 2. Провести инвентаризацию всей инфраструктуры, использующей PHP, включая веб-серверы, панели управления и стороннее ПО. 3. При невозможности обновления применить временные компенсирующие меры: отключить механизм session.upload_progress (session.upload_progress.enabled = Off) и ограничить обработку multipart-запросов на уровне веб-сервера. 4. Провести проверку корпоративной инфраструктуры на наличие признаков компрометации на предмет аномальной активности веб-приложений. 5. Обеспечить мониторинг попыток эксплуатации уязвимостей средствами защиты информации и антивирусной защиты с актуальными базами.