ЭТИ 3 УЯЗВИМОСТИ СДЕЛАЛИ САЙТЫ УЯЗВИМЫМИ

PHP2Shell
CVE-2026-109618
CVE-2026-109619
php
ВОЗМОЖЕН ЗАХВАТ СИСТЕМЫ

Node2Shell
CVE-2026-111497
node JS
ВОЗМОЖНО УДАЛЁННОЕ ВЫПОЛНЕНИЕ КОДА

HTTP2Shell
CVE-2026-111497
(та же первопричина)
HTTP/2
УДАЛЁННОЕ ВЫПОЛНЕНИЕ КОДА

@lionsoulbatyshchikov

PHP2Shell / CVE-2026-109618 CVE-2026-109619

PHP2SHELL

ДВЕ КРИТИЧЕСКИЕ УЯЗВИМОСТИ В САМОМ PHP.

Специально сформированный HTTP-запрос может привести к повреждению памяти и потенциальному удалённому выполнению кода (RCE).

1 CVE-2026-109618 — ПЕРЕПОЛНЕНИЕ ПАМЯТИ (OUT-OF-MEMORY)

Возникает, когда PHP обрабатывает специально сформированный запрос.

1 СПЕЦИАЛЬНЫЙ ЗАПРОС

Атакующий отправляет особый HTTP-запрос.

```
POST /index.php HTTP/1.1
Host: target.com
Content-Type: multipart/
form-data; boundary=------
-------

(вредоносные данные)
```

2 ИСТОЩЕНИЕ ПАМЯТИ

Запрос заставляет PHP выделять большие объёмы памяти, что приводит к out-of-memory.



ПРЕВЫШЕН ЛИМИТ ПАМЯТИ

3 ОШИБКА ОБРАБОТКИ

Неверная обработка ошибки в PHP оставляет частично инициализированную память.



НЕКОРРЕКТНАЯ ОЧИСТКА ПАМЯТИ

4 ПОВРЕЖДЕНИЕ ПАМЯТИ

При определённых условиях это приводит к повреждению памяти и может дать удалённое выполнение кода (RCE).

```
$ whoami
www-data
```

2 CVE-2026-109619 — ИСПОЛЬЗОВАНИЕ ОСВОБОЖДЁННОЙ ПАМЯТИ (USE-AFTER-FREE)

Возникает во время обработки сессии или загрузки файла, когда остаётся висячая ссылка (stale reference).

1 ВЫЗОВ ОШИБКИ

Специальный запрос вызывает ошибку при обработке сессии или загрузке файла.

```
POST /upload.php HTTP/1.1
Host: target.com
Content-Type: multipart/
form-data; boundary=------

(некорректные данные)
```

2 ПАМЯТЬ ОСВОБОЖДАЕТСЯ

PHP освобождает блок памяти, но оставляет висячую ссылку (pointer).



3 ПОВТОРНОЕ ИСПОЛЬЗОВАНИЕ

Позже другой запрос, обработанный тем же потоком/воркером, может переиспользовать этот освобождённый блок.



Атакующий контролирует новые данные

4 ВОЗМОЖНОСТЬ RCE

Манипулируя переиспользованной памятью, атакующий может добиться удалённого выполнения кода.

```
$ id
uid=33(www-data)
gid=33(www-data)
```

ПОЧЕМУ ЭТО ВАЖНО?

Уязвимость находится в самом PHP — а не в WordPress, плагинах или коде вашего сайта.

ГДЕ ЕСТЬ РИСК?

Под угрозой сайты, веб-приложения и сервисы, работающие на уязвимых версиях PHP, в зависимости от конфигурации и поверхности атаки.

@lionsoulbatyshchikov

Node2Shell / CVE-2026-111497

NODE2SHELL

УЯЗВИМОСТЬ СЖАТИЯ, КОТОРАЯ МОЖЕТ ПРИВЕСТИ К RCE.

Уязвимость в декодере Brotli, используемом в Node.js, может быть вызвана специально созданными сжатыми данными, что приводит к повреждению памяти и потенциальному удалённому выполнению кода (RCE).



КАК ЭТО РАБОТАЕТ?

Специально сформированные Brotli-сжатые данные могут вызвать выход за границы буфера (out-of-bounds write) в декодере.

1 СПЕЦИАЛЬНЫЕ ДАННЫЕ

Атакующий отправляет вредоносные сжатые данные (например, через HTTP-запрос, загрузку файла или любой функционал, где происходит декомпрессия).

```
POST /upload HTTP/1.1
Host: target.com
Content-Encoding: br
Content-Type: application/
octet-stream

(вредоносные Brotli данные)
8b 1f 00 00 00 00 00 00
ff ff ff ...
```

2 ДЕКОДЕР BROTLI

Node.js использует встроенный Brotli decoder для распаковки данных.

Brotli Decoder

Используется внутри Node.js

- HTTP (Content-Encoding)
- Обработка файлов
- Фреймворки и библиотеки
- Сторонние пакеты
- Любой функционал, работающий со сжатыми Brotli данными

3 ПОВРЕЖДЕНИЕ ПАМЯТИ

Ошибка в декодере позволяет записать данные за пределами выделенного буфера при обработке специально созданных данных.



4 ВОЗМОЖНЫЕ ПОСЛЕДСТВИЯ

Это может привести к сбою, утечке данных из памяти и потенциальному удалённому выполнению кода (RCE) — в зависимости от приложения и условий.

```
$ whoami
www-data

$ id
uid=33(www-data)
gid=33(www-data)
```

ГДЕ ЭТО МОЖЕТ ВСТРЕТИТЬСЯ?

Не только прямое использование. Многие приложения могут быть уязвимы через зависимости и автоматическую декомпрессию.

- **HTTP-серверы** (Content-Encoding: br)
- **Функции загрузки файлов**
- **Фреймворки** (Express и др.)
- **NPM пакеты**, использующие Brotli
- **Обратные прокси и API gateways**
- **Приложения**, обрабатывающие сжатые данные

КЛЮЧЕВЫЕ ВЫВОДЫ

- Обновите Node.js до исправленной версии.
- Проверьте приложения и зависимости, которые используют Brotli.
- Проведите аудит функционала, работающего со сжатыми данными (загрузка файлов, HTTP, API).
- Убедитесь, что патчи применены во всех окружениях (контейнеры, CI/CD, production).

@lionsoulbatyshchikov

HTTP2Shell / CVE-2026-111497 (та же уязвимость)

HTTP2SHELL

ДРУГОЕ НАЗВАНИЕ. ТА ЖЕ ОПАСНАЯ УЯЗВИМОСТЬ.

HTTP2Shell — это то же самое, что и уязвимость в декодере Brotli (CVE-2026-111497), отслеживаемая как Node2Shell. Её можно вызвать через HTTP-запросы с вредоносно подготовленными сжатыми данными.



КАК ПРОХОДИТ АТАКА?

Вредоносные Brotli-сжатые данные отправляются через HTTP-запрос, обрабатываются уязвимым декодером и могут привести к повреждению памяти и потенциальному удалённому выполнению кода (RCE).

1 ПОДГОТОВКА ВРЕДОНОСНЫХ ДАННЫХ

Атакующий создаёт специально сформированные Brotli-сжатые данные с вредоносным содержимым.

```
HTTP Request
POST /upload HTTP/2
Host: target.com
Content-Encoding: br
Content-Type: data

(вредоносные Brotli данные)
```

2 ОТПРАВКА ЧЕРЕЗ HTTP/2

Данные отправляются в виде HTTP/2 запроса (например, загрузка файла, вызов API или любой эндпоинт, принимающий сжатые данные).



Вредоносные Brotli-сжатые данные

3 УЯЗВИМЫЙ ДЕКОДЕР BROTLI

Приложение автоматически распаковывает данные с помощью уязвимого **Brotli decoder** (та же уязвимость, что и Node2Shell).



CVE-2026-111497

4 ПОВРЕЖДЕНИЕ ПАМЯТИ

Ошибка в декодере позволяет записать данные за пределами буфера (out-of-bounds write) при обработке некорректных данных.



Запись за пределы границ памяти

5 ВОЗМОЖНОСТЬ RCE

Это может привести к падению приложения, утечке данных или потенциальному удалённому выполнению кода (RCE) — в зависимости от окружения и условий.

```
$ whoami
www-data
$ id
uid=33(www-data)
gid=33(www-data)
```

ГДЕ ЭТО МОЖЕТ ВСТРЕТИТЬСЯ?

Уязвимый компонент Brotli используется не только в Node.js, но и в других программных экосистемах.

- **Node.js** (Runtime & Packages)
- **.NET** (ASP.NET, Kestrel и др.)
- **Python** (различные пакеты)
- **Web-серверы** (HTTP/2, прокси)
- **Фреймворки** (Express, Fastify и др.)
- **Другие интеграции** (любое ПО, использующее Brotli библиотеки)

КЛЮЧЕВЫЕ ВЫВОДЫ

HTTP2Shell — не отдельная уязвимость.
Это то же самое, что и уязвимость в декодере Brotli (CVE-2026-111497), отслеживаемая как Node2Shell.

Доступна через HTTP-запросы.
Любое приложение, автоматически распаковывающее Brotli-данные, может быть под угрозой.

Проверьте зависимости.
Обновите Node.js, .NET, Python пакеты и другое ПО, использующее уязвимые Brotli библиотеки.

Убедитесь, что патчи применены.
Проверьте все окружения (контейнеры, CI/CD, production) и обновите версии.

@lionsoulbatyshchikov

ЧТО НУЖНО СДЕЛАТЬ

- Определите затронутые версии
- Установите обновления
- Проверьте окружение
- Следите за признаками эксплуатации

ПРОВЕРИТЬ / ОБНОВИТЬ / ЗАЩИТИТЬ / БЫТЬ ГОТОВЫМ

PHP2Shell

CVE-2026-109618
CVE-2026-109619

Проверьте версию PHP
Убедитесь, что не используете уязвимые версии.

Обновите до исправленных версий
Установите патчи, выпущенные PHP project.

Проверьте ваши приложения
Убедитесь, что они корректно работают после обновления.

Мониторьте логи
Ищите подозрительные запросы и аномальное поведение.

ЧАСТО ЗАТРАГИВАЕТ

Self-hosted PHP, приложения, фреймворки и сервисы, работающие на уязвимых версиях PHP.

Node2Shell

CVE-2026-111497

Проверьте версию Node.js
Обновитесь до исправленной LTS или актуальной версии.

Обновите зависимости
Проверьте и обновите пакеты, которые используют уязвимый Brotli.

Проведите аудит обработки данных
Проверьте загрузку файлов, API endpoints и другие функции, работающие со сжатыми данными.

Мониторьте и выявляйте
Ищите сбои, необычное использование памяти и подозрительную активность.

ЧАСТО ЗАТРАГИВАЕТ

Node.js приложения, фреймворки и сервисы, обрабатывающие Brotli-сжатые данные.

HTTP2Shell

CVE-2026-111497

Проверьте ПО, использующее Brotli
Веб-серверы, фреймворки, библиотеки и прокси.

Обновите до исправленных версий
Установите патчи для компонента Brotli.

Проверьте HTTP endpoints
Любой endpoint, принимающий сжатые данные, может быть уязвим.

Проверьте в проде
Убедитесь, что все контейнеры, CI/CD пайплайны и серверы обновлены.

ЧАСТО ЗАТРАГИВАЕТ

Веб-серверы, фреймворки, библиотеки и другое ПО, использующее уязвимый Brotli decoder.

- Web Servers (HTTP/2)
- Frameworks (Express и др.)
- Другой софт (.NET, Python и др.)

@lionsoulbatyshchikov