AIRNITE

# ZERO DAY

العدد 02/2026 · أمن المعلومات

# باب خلفي في نواة PHP: كيف تلاعب المهاجمون بالشيفرة المصدرية للغة الويب

في مارس 2021 وصل إيداعان (commits) جرى التلاعب بهما إلى الشيفرة المصدرية الرسمية لـ PHP، متخفّيين تحت أسماء مطوّرين معروفين. كيف عمل الباب الخلفي، وما الذي ينبغي لكل فريق برمجيات أن يتعلمه منه.

---

تاريخ النشر: 21 نوفمبر 2026 مدة القراءة: 6 دقيقة الكاتب: فريق تحرير Airnite

| 2 | 11 | 0 | 2FA |
|---|---|---|---|
| **إيداعان جرى التلاعب بهما** | **سطرًا من الشيفرة الخبيثة** | **حاجة إلى تسجيل الدخول** | **شرط لصلاحيات الكتابة** |
| باسمَي Rasmus Lerdorf وNikita Popov (php.internals، 28 مارس 2021) | في ext/zlib/zlib.c، متنكّرة في صورة «Fix typo» (GitHub) | تنفيذ الشيفرة عبر ترويسة HTTP لأي زائر (محتوى الإيداع) | منذ ذلك الحين عبر مؤسسة PHP على GitHub فقط (php.internals) |

تدخل PHP في كثير من أنظمة إدارة المحتوى والمتاجر الإلكترونية وبوابات العملاء. وفي 28 مارس 2021 ظهر في مستودع الشيفرة المصدرية الرسمي لمشروع PHP تغييران بدَوَا غير مؤذيين. وحمل أحدهما عنوان «Fix typo». لكنه في الحقيقة زرع بابًا خلفيًا يتيح تنفيذ أي شيفرة على كل خادم يعمل بإصدار PHP معدّل على هذا النحو.

## // ماذا حدث؟

وفقًا لما أعلنه Nikita Popov، أحد المطوّرين الأساسيين لـ PHP، على القائمة البريدية php.internals، جرى دسّ إيداعين خبيثين في مستودع php-src، أحدهما باسم مبتكر PHP **Rasmus Lerdorf**، والآخر باسم Popov نفسه. وبحسب ESET، لُفت الانتباه إلى التغيير الأول خلال مراجعة روتينية بعد الإيداع، فجرى التراجع عنه سريعًا؛ إذ تساءل مطوّرون من المجتمع عمّا تفعله هذه الشيفرة أصلًا.

وجاء ردّ المشروع جذريًا. فقد تقرر التوقف عن استخدام خادم Git الخاص بالمشروع git.php.net، وأصبحت النسخ المتطابقة السابقة على **GitHub** هي المصدر المعتمد. ومنذ ذلك الحين لا تُمنح صلاحيات الكتابة إلا لأعضاء مؤسسة PHP على GitHub، وهي تشترط **المصادقة الثنائية**. وظهر في نص الإيداع اسم «Zerodium»، وهي جهة تتاجر بالثغرات الأمنية؛ وبحسب ESET نفى رئيسها أي تورط.

## // كيف يعمل الهجوم؟

تتألف الشيفرة الخبيثة من أحد عشر سطرًا في الملف المسؤول عن ضغط zlib. وهي تقرأ ترويسة HTTP تحمل اسمًا لا يكاد يلفت النظر هو **«User-Agentt»** (بحرف t مكرر). فإذا بدأت قيمتها بكلمة «zerodium»، نفّذت PHP بقية الترويسة على أنها شيفرة برمجية. أي أن المهاجم لم يكن يحتاج إلا إلى إرسال طلب مُعَدّ بعناية إلى موقع إلكتروني، من دون تسجيل دخول ومن دون كلمة مرور.

أما كيف تمكّن المهاجمون من الكتابة، فقد أوضحه تحديث صدر في 6 أبريل 2021. فبحسبه لم يعد الفريق يعتقد أن خادم Git قد اختُرق. فالتغييرات رُفعت عبر HTTPS بتسجيل دخول بكلمة مرور يُتحقق منها مقابل قاعدة بيانات المستخدمين في master.php.net، ومن المحتمل أن تكون هذه القاعدة قد سُرّبت. فانتقل الفريق إلى خوارزميات تجزئة حديثة لكلمات المرور، وأعاد تعيين **جميع كلمات مرور php.net**، وأعاد بناء الخادم.

## // من المتأثر؟

لم يستهدف الهجوم شركة بعينها، بل **سلسلة توريد البرمجيات**: فمن يتلاعب بالشيفرة عند مصدرها يصل إلى كل من يعتمدها لاحقًا. وكان اكتشاف الباب الخلفي مبكرًا بفضل مراجعين يقظين، لا بفضل حاجز تقني. وبحسب Popov، في ما نقلته ESET، أُزيل التغيير قبل أن يصل إلى بيئات التشغيل الفعلية.

وينطبق هذا النمط على كل شركة تطوّر برمجياتها الخاصة أو تستخدم مكتبات خارجية. فالخوادم القديمة المُدارة ذاتيًا بنظام مستخدمين خاص، وتسجيل الدخول بكلمة مرور دون عامل ثانٍ، والثقة بالأسماء المعروفة في سجل الإيداعات، هي بالضبط نقاط الضعف التي استُغلّت هنا. فوجود اسم على إيداع لا يثبت من كتبه فعلًا.

## // ما الذي يجب فعله الآن؟

إجراءات PHP نموذج جيد يُحتذى: إدارة صلاحيات الكتابة مركزيًا، وجعل المصادقة الثنائية إلزامية، وإيقاف الأنظمة القديمة، وتخزين كلمات المرور بأمان. ويُضاف إلى ذلك إجراء مراجعة يأخذ التغييرات الصغيرة أيضًا على محمل الجد. فالباب الخلفي كان متنكّرًا في صورة تصحيح لخطأ مطبعي، وهذا النوع من الإيداعات بالذات كثيرًا ما يُمرَّر دون تدقيق.

ومن يستخدم برمجيات خارجية ينبغي أن يعرف مصدر كل مكوّن، وأن يحصل على التحديثات من مصادر محددة مسبقًا. وتلخّص قائمة التحقق أدناه أهم الخطوات.

## // كيف تساعدكم Airnite؟

تطوّر Airnite **برمجيات** بسلسلة توريد سليمة: مستودعات محمية، ومراجعات إلزامية، وإيداعات موقّعة، وفحص للاعتماديات في مسار البناء. وفي **اختبار الاختراق** نتحقق مما إذا كانت حسابات المطوّرين وخوادم Git وأنظمة البناء قابلة للاختراق من الخارج. وفي **الاستشارات** نبيّن لفريقكم كيف يعتمد إجراءات تكشف مثل هذه التلاعبات مبكرًا.

> ملاحظة: مقال تأسيسي حول حادثة وقعت عام 2021، وتُعدّ مثالًا تعليميًا على الهجمات التي تستهدف سلسلة توريد البرمجيات. تاريخ البحث: 21 نوفمبر 2026.

## قائمة التحقق: ما ينبغي لكم فعله الآن

- [+] منح صلاحيات الكتابة في مستودعات الشيفرة عبر حسابات مُدارة مركزيًا ومحمية بالمصادقة الثنائية فقط، وإيقاف الخوادم ومسارات الوصول القديمة.
- [+] اعتماد كل تغيير على الفرع الرئيسي عبر طلب سحب (Pull Request) ومراجعة من شخص ثانٍ، بما في ذلك «تصحيحات الأخطاء المطبعية».
- [+] توقيع الإيداعات والتحقق من التواقيع في مسار البناء.
- [+] البحث المتعمّد أثناء المراجعة عن الأنماط المريبة: استدعاءات eval، وأسماء ترويسات غير مألوفة، وشيفرة داخل وحدات الضغط أو تسجيل الأحداث.
- [+] حماية قواعد بيانات كلمات المرور الخاصة بحسابات المطوّرين بخوارزميات تجزئة حديثة، وإعادة تعيين جميع كلمات المرور بعد أي حادثة.
- [+] حصر الاعتماديات الخاصة بكم (SBOM) وعدم الحصول عليها إلا من مصادر موثوقة ومحددة مسبقًا.

## كيف تساعدكم Airnite

- البرمجيات والمواقع الإلكترونية – مواقع إلكترونية وتطبيقات ويب سريعة وآمنة ومتعددة اللغات.
- اختبار الاختراق والأمن – هجمات منضبطة مع تقرير واضح وخطة إجراءات.
- الاستشارات – نظرة خارجية على خططكم ومشاريعكم.

### ما مدى أمان سلسلة توريد البرمجيات لديكم؟

تفحص Airnite من يملك صلاحية الكتابة في مستودعاتكم، وكيف تُعتمد التغييرات، وأي حزم خارجية تدخل إلى برمجياتكم. وتحصلون على قائمة واضحة بالثغرات والإجراءات، من إلزامية المصادقة الثنائية إلى الإيداعات الموقّعة وفحص الاعتماديات.

**اطلبوا محادثة أولية · راسلونا بالبريد الإلكتروني · عبر WhatsApp**

### اتصل بنا

لديكم أسئلة حول هذا المقال؟ راسلونا عبر WhatsApp: +49 174 6834842

اقرؤوه على الإنترنت: https://airnite.de/ar/magazine/php-source-code-backdoor-git-server/

## المصادر

تستند كل معلومة في هذا المقال إلى المصادر التالية. المصادر الأولية مميّزة.


1. **php.internals · Nikita Popov: Changes to Git commit workflow** مارس 2021 · مصدر أولي · 28
   مصدر أولي: إيداعان جرى التلاعب بهما، والاشتباه في اختراق git.php.net، والانتقال إلى GitHub، وإلزامية 2FA
   https://news-web.php.net/php.internals/113838
2. **php.internals · Nikita Popov: Update on git.php.net incident** أبريل 2021 · مصدر أولي · 6
   مصدر أولي: الخادم لم يُخترق على الأرجح، واحتمال تسريب قاعدة بيانات المستخدمين، وإعادة تعيين كلمات المرور
   https://news-web.php.net/php.internals/113981
3. **GitHub · الإيداع c730aa2 في php/php-src «[skip-ci] Fix typo»** مارس 2021 · مصدر أولي · 28
   مصدر أولي: محتوى الشيفرة الخبيثة في ext/zlib/zlib.c
   https://github.com/php/php-src/commit/c730aa26bd52829a49f2ad284b181b7e82a68d7d
4. **ESET WeLiveSecurity · Backdoor added to PHP source code in Git server breach** مارس 2021 · 30
   بحث أمني: الاكتشاف أثناء المراجعة، وشرح آلية العمل، ونفي Zerodium
   https://www.welivesecurity.com/2021/03/30/backdoor-php-source-code-git-server-breach/


*معلومات تحريرية عامة، وليست استشارة قانونية ولا فحصًا فرديًا لأنظمتكم. الحالة: تاريخ النشر.*


Airnite GmbH · Am Waldbach 7 · 77654 Offenburg · airnite.de