Apache HTTP Server يعالج ثغرة حرجة في HTTP/2 تتيح تنفيذ الأوامر عن بُعد (CVE-2026-119618)



أصلحت Apache الثغرة CVE-2026-119618، وهي حالة تعارض في mod_http2 تتيح لمهاجم غير موثّق تنفيذ تعليمات برمجية عن بُعد. يُنصح بالتحديث أو تعطيل HTTP/2 مؤقتًا.

- الثغرة CVE-2026-119618 حالة تعارض في mod_http2 تُفسد ذاكرة الكومة وقد تؤدي إلى تنفيذ تعليمات عن بُعد دون مصادقة.
- الإصدارات المتأثرة: Apache HTTP Server من 2.4.55 إلى 2.4.70، وmod_h2 المستقل من 2.0.8 إلى 2.0.42.
- يتطلب الاستغلال تفعيل HTTP/2، وهو معطّل افتراضيًا.
- تفيد بيانات Wiz بأن 64% من البيئات السحابية تضم موارد معرّضة، ونحو نصفها مكشوف للإنترنت؛ ولا علم لـ Wiz بأي استغلال علني حتى الآن.
- يعالج الإصدار الأحدث أيضًا الثغرة CVE-2026-106023 في mod_md وثغرة منخفضة الخطورة

> CVE-2026-109163 في mod_vhost_alias.

أصدرت مؤسسة Apache Software Foundation إصلاحًا لثغرة حرجة في وحدة HTTP/2 ضمن Apache HTTP Server، تحمل الرقم CVE-2026-119618، ويمكن لمهاجم غير موثّق استغلالها لتنفيذ تعليمات برمجية عن بُعد.

طبيعة الثغرة

تتمثل المشكلة في حالة تعارض (race condition) داخل وحدة mod_http2 ناجمة عن ضعف التزامن بين مسارات تنفيذ متزامنة تتشارك الموارد. وقد تُفسد ذاكرة الكومة، ووفق باحثي Wiz يمكن توظيف ذلك لتنفيذ أوامر اعتباطية بصلاحيات عملية خادم الويب. تشمل الثغرة Apache HTTP Server من الإصدار 2.4.55 إلى 2.4.70، وmod_h2 المستقل من 2.0.8 إلى 2.0.42. اكتشفها فريقا Anthropic's OSS Scanner وGoogle Cloud Vulnerability Research.

حجم التعرض والوضع الحالي

تشير بيانات Wiz إلى أن 64% من البيئات السحابية تحتوي موارد معرّضة، وأن نحو نصفها له نسخ مكشوفة للإنترنت. ولا تأخذ هذه الأرقام في الحسبان الإعدادات، إذ يشترط الاستغلال تفعيل HTTP/2 وهو معطّل افتراضيًا. وأكدت watchTowr هذا الشرط، ونصحت بالتحديث فورًا أو تعطيل h2 إلى حين ذلك.

تصنّف Wiz الخطورة بأنها حرجة رغم عدم وجود تقييم رسمي، وتفيد بعدم علمها بأي استغلال علني أو هجمات، لكنها تحذّر من أن الوضع قد يتغير قريبًا. كما يعالج الإصدار نفسه الثغرة CVE-2026-106023 في mod_md، والثغرة منخفضة الخطورة CVE-2026-109163 في mod_vhost_alias.

على الجهات التي تشغّل Apache على أنظمة متصلة بالإنترنت التحقق سريعًا من الإصدارات وإعدادات HTTP/2.

ما يجب فعله الآن

1. حصر جميع نسخ Apache HTTP Server وmod_h2 المستقل، بما في ذلك البيئات السحابية والمستضافة لدى أطراف ثالثة، وتوثيق الإصدارات.
2. تحديث الخوادم المتأثرة إلى أحدث إصدار من Apache HTTP Server مع إعطاء الأولوية للأنظمة المتصلة بالإنترنت.
3. تعطيل HTTP/2 مؤقتًا حيث يتعذر التحديث الفوري، إلى حين تطبيقه.
4. مراجعة الإعدادات لمعرفة ما إذا كان HTTP/2 مفعّلاً على كل خادم.
5. مراقبة خوادم الويب بحثًا عن نشاط غير معتاد للعمليات أو أوامر غير متوقعة، ومراجعة السجلات لرصد أي مؤشرات اختراق.
6. توثيق التعرض والمعالجة ضمن إدارة الثغرات لتوفير أدلة الامتثال لضوابط الأمن السيبراني (ECC) وإطار SAMA CSF.