دروبال تصدر تحديثات لإصلاح ثغرة حرجة تتيح تنفيذ تعليمات برمجية عن بُعد عبر الوحدات المساهمة

أصدرت دروبال تحديثات أمنية في 14 أكتوبر لمعالجة ثغرة حرجة في وحدة Field UI تتيح تنفيذ تعليمات برمجية عن بُعد، مع وجود مسار استغلال معروف لا يتطلب مصادقة.

- أصدرت دروبال تحديثات أمنية في 14 أكتوبر 2024 للإصدارات 11.4.10 و11.3.19 و10.6.19 لمعالجة ثغرة حرجة في وحدة Field UI
- تتيح الثغرة تنفيذ تعليمات برمجية عن بُعد على الخادم المستضيف لموقع دروبال
- لا يمكن استغلال الثغرة من خلال نواة دروبال وحدها بل تتطلب وحدات مساهمة لإنشاء مسارات الاستغلال
- يوجد مسار استغلال معروف واحد على الأقل لا يتطلب مصادقة المهاجم
- تم تحديد مسارات استغلال متعددة عبر وحدات مساهمة مختلفة

تفاصيل الثغرة الأمنية

أصدرت دروبال تحديثات أمنية في 14 أكتوبر 2024 لمعالجة ثغرة حرجة في **وحدة Field UI**، وهي مكون من مكونات نواة دروبال. تتيح الثغرة تنفيذ تعليمات برمجية عن بُعد على الخادم المستضيف لتثبيت دروبال المتأثر. الإصدارات المحدثة هي 11.4.10 و11.3.19 و10.6.19.

وفقاً للتنبيه الصادر عن فريق الأمن في دروبال، لا يمكن استغلال الثغرة من خلال وظائف نواة دروبال وحدها. بدلًا من ذلك، يجب على المهاجمين الاستفادة من الوحدات المساهمة - وهي إضافات طورها مجتمع دروبال - لإنشاء مسارات استغلال قابلة للتطبيق. أكد فريق الأمن وجود مسارات متعددة من هذا القبيل عبر وحدات مساهمة مختلفة.

عدم الحاجة للمصادقة لاستغلال الثغرة

الجانب المثير للقلق بشكل خاص في هذه الثغرة هو أن مساراً واحداً معروفاً على الأقل لا يتطلب من المهاجم المصادقة على النظام. هذا يخفض بشكل كبير حاجز الاستغلال ويزيد من مستوى المخاطر لتثبيتات دروبال المتاحة للعموم والتي تستخدم وحدات مساهمة ضعيفة إلى جانب إصدارات النواة المتأثرة.

إن الجمع بين الخطورة الحرجة وقدرة تنفيذ التعليمات البرمجية عن بُعد والوصول غير المصادق يجعل من هذه الثغرة أولوية للمعالجة الفورية. يجب على المؤسسات التي تدير مواقع دروبال التحقق من إصدار النواة ومراجعة الوحدات المساهمة المثبتة لتقييم مدى التعرض.

توفر التحديثات

أصدرت دروبال إصلاحات عبر ثلاثة فروع إصدار مدعومة. يجب على المؤسسات تطبيق التحديث المناسب بناءً على إصدارها الرئيسي الحالي: 11.4.10 لفرع 11.4.x الأحدث، و11.3.19 لفرع 11.3.x، و10.6.19 للمواقع التي لا تزال تعمل بدروبال 10. لم يكشف فريق الأمن عن تفاصيل محددة حول الوحدات المساهمة الضعيفة أو تقنيات الاستغلال لمنع الاستغلال الواسع النطاق قبل اكتمال التحديث.

ما يجب فعله الآن

1. تحديد جميع تثبيتات دروبال عبر البنية التحتية الإلكترونية للمؤسسة وتوثيق إصداراتها الحالية
2. تطبيق التحديثات الأمنية فوراً للترقية إلى دروبال 11.4.10 أو 11.3.19 أو 10.6.19 حسب الإصدار الرئيسي الحالي
3. إجراء جرد لجميع الوحدات المساهمة المثبتة على كل نسخة دروبال وتقييم ضرورتها
4. مراجعة قواعد جدار حماية تطبيقات الويب وتوقيعات كشف التطفل لرصد محاولات الاستغلال المحتملة المستهدفة لوحدة Field UI في دروبال
5. متابعة التنبيهات الأمنية من دروبال للحصول على تحديثات حول الوحدات المساهمة الضعيفة عند توفر التفاصيل
6. جدولة اختبارات اختراق لمواقع دروبال المتاحة للعموم للتحقق من فعالية التحديثات وتحديد التعرض المتبقي