

ثغرة حقن أوامر في Apache Struts تتطلب تطبيق التحديثات الأمنية فوراً



يحتوي Apache Struts على ثغرة حقن أوامر تمكّن المهاجمين عن بُعد من تنفيذ أكواد عشوائية عند تفعيل Dynamic Method Invocation، مما يستوجب تطبيق تحديثات البائع فوراً.

• Apache Struts عرضة لحقن أوامر عن بُعد عبر method:prefix عند تفعيل Dynamic Method Invocation

- يمكن للمهاجمين تنفيذ أكواد عشوائية عن بُعد دون مصادقة
- يجب تطبيق تحديثات وإجراءات البائع الوقائية فوراً
- على المؤسسات تقييم مدى تعرض الأصول المتأثرة للإنترنت
- يجب إيقاف استخدام المنتج في حال عدم توفر إجراءات وقائية

نظرة عامة على الثغرة

يحتوي Apache Struts على **ثغرة حقن أوامر** مسجلة برقم CVE-2016-3081 تسمح للمهاجمين عن بُعد بتنفيذ أكواد عشوائية على الأنظمة المتأثرة. يمكن استغلال الثغرة من خلال آلية `method:prefix` عند تفعيل **Dynamic Method Invocation** في إعدادات التطبيق. تتيح هذه الثغرة للمهاجمين غير المصادق عليهم حقن وتنفيذ أوامر ضارة عن بُعد، مما يشكل خطراً كبيراً على تطبيقات الويب المبنية على إصدارات Struts المعرضة للخطر.

المخاطر على المؤسسات الخاضعة للتنظيم

تواجه المؤسسات التي تشغل تطبيقات مبنية على Apache Struts تعرضاً فورياً لهجمات تنفيذ الأكواد عن بُعد. لا تتطلب الثغرة أي مصادقة، مما يجعلها خطيرة بشكل خاص للتطبيقات المتصلة بالإنترنت الشائعة في القطاعات المصرفية والصحية والحكومية. قد يؤدي الاستغلال الناجح إلى اختراق كامل للنظام وانتهاكات للبيانات وعدم الامتثال التنظيمي.

الاستجابة المطلوبة

يجب على المؤسسات تطبيق التحديثات والإجراءات الوقائية المقدمة من البائع دون تأخير. ينبغي على المؤسسات إجراء جرد لجميع عمليات نشر Apache Struts وتقييم تعرضها للإنترنت وترتيب أولويات التحديث بناءً على المخاطر. في حال عدم توفر إجراءات وقائية، يجب فصل التطبيقات المتأثرة عن الشبكة أو إيقافها. تتطلب تطبيقات Struts المستضافة سحابياً التنسيق مع مزودي الخدمة لضمان تطبيق التحديثات. يجب على المؤسسات غير القادرة على التحديث فوراً تطبيق ضوابط تعويضية ومراقبة الأنظمة المتأثرة لرصد علامات الاستغلال.

ما يجب فعله الآن

1. إجراء جرد فوري لجميع عمليات نشر Apache Struts في بيئتك
2. تطبيق التحديثات الأمنية المقدمة من البائع على جميع تبيئات Struts المتأثرة
3. تعطيل Dynamic Method Invocation في ملفات إعدادات Struts حيثما لا يكون مطلوباً تشغيلياً
4. تقييم مدى تعرض جميع التطبيقات المبنية على Struts للإنترنت وترتيب أولويات التحديث وفقاً لذلك
5. تطبيق تجزئة الشبكة وضوابط الوصول للحد من تعرض الأنظمة المعرضة للخطر
6. مراقبة سجلات التطبيقات وحركة الشبكة لرصد مؤشرات محاولات الاستغلال
7. التنسيق مع مزودي الخدمات السحابية لضمان تطبيق التحديثات على تطبيقات Struts المستضافة
8. إيقاف استخدام التطبيقات المتأثرة أو فصلها عن الشبكة في حال تعذر تطبيق التحديثات فوراً