اختراق أوبر يظهر ضعف خدمات مشاركة التعليمات البرمجية

الثلاثاء 28 نوفمبر 2017 09:11 م

أظهرت عملية اختراق بيانات شركة خدمات الركوب أوبر ضعف برمجيات خدمات مشاركة التعليمات البرمجية وحملت في طياتها درساً لمطوري البرمجيات الذين يستخدمون مثل هذه الخدمات التابعة لطرف ثالث من أجل تخزين ومشاركة وتبادل التعليمات البرمجية مفاده الحذر حول ما يقومون بمشاركته

ويجري استعمال خدمات مثل شركة Github ومقرها سان فرانسيسكو وGitLab وSourceForge من قبل المطورين للتعاون فيما بينهم ضمن المشاريع وتتبع الأخطاء في التعليمات البرمجية وتوزيع الإصدارات المبكرة من التطبيقات، كما تعتبر تلك الخدمات بمثابة أهدف للصوص الإنترنت

وفقدت شركة أوبر معلومات شخصية لنحو 57 مليون حساب من حسابات مستخدمي وسائقي أكبر شركة لخدمات الركوب والنقل التشاركي في العالم، وذلك بعد تمكن الهاكرز من الوصول إلى منطقة محمية بكلمة مرور في خدمة Github، والتي تعتبر واحدة من أكبر مخازن التعليمات البرمجية شعبية في العالم

وقال كريس بويد المحلل في شركة الأمن السيبراني Malwarebytes "يمكن أن تكون عمليات تخزين وحفظ التعليمات البرمجية مشكلة كبيرة جداً"، حيث تعاني العديد من الشركات من بطء في عملية إزالة تفاصيل تسجيل الدخول إلى هذه الخدمات التخزينية عند مغادرة المطورين

وقد وجد باحث أمني في وقت سابق من هذا الشهر بأن مطوري البرمجيات التابعين للشركة الصينية المصنعة للطائرات بدون طيار DJI Technology قد قاموا بترك المفاتيح الخاصة لحساباتهم السحابية في خدمة أمازون AWS وجميع مواقع الشركة ضمن تعليمات برمجية قاموا بنشرها علناً ضمن خدمة Github.

كما تمكنت مجموعة من الهاكرز في عام 2014 من العثور على مفتاح تسجيل الدخول موجوداً ضمن التعليمات البرمجية التي قام مطورو أوبر بنشرها علناً ضمن Github، مما أدى إلى سرقة بيانات نحو 50 ألف من سائقي خدمة أوبر

ورفعت شركة خدمات الركوب في عام 2015 دعوى قضائية ضد Github لإرغام الخدمة على تسليم المعلومات المتعلقة بالمستخدمين الذين قد يكونوا وصلوا إلى المنطقة التي تواجدت فيها التعليمات البرمجية

وأوضح ادوين فوديل الباحث الأمني المعروف بالاسم الرمزي EdOverflow بأن العديد من الشركات تعمل عن طريق الخطأ على إضافة كلمات السر والمفاتيح الخاصة في التعليمات البرمجية التي تنشر على خدمات التخزين، وقال "هذا الأمر منتشر بشكل لا يصدق"، مضيفاً بأن بعض المطورين يفترضون أن التعليمات البرمجية الخاصة بهم آمنة عندما تكون في منطقة محمية بكلمة مرور

ويعمد الهاكرز الباحثين عن نقاط الضعف إلى القيام بمراجعة روتينية للتعليمات البرمجية المنشورة علناً ضمن Github من أجل الوصول إلى كلمات السر ومفاتيح التشفير الخاصة التي تركت من قبل المطورين بشكل مرئي

ورفضت خدمة Github التعليق على الحسابات الفردية عندما تم سؤالها فيما يخص أحدث اختراق لخدمة أوبر، واكتفت بالقول بأنها تنصح المستخدمين بعدم تخزين رموز الوصول وكلمات السر أو غيرها من بيانات المصادقة أو مفاتيح التشفير ضمن التعليمات البرمجية، وأنه يجب على المطورين استعمال إجراءات أمنية إضافية في حال كان يجب عليهم تضمين مثل هذه العناصر من أجل منع الوصول غير المصرح به أو إساءة الاستعمال

وتستعمل مجموعة 18F، وهي مجموعة من المبرمجين الذين يساعدون في بناء البرمجيات للحكومة الأمريكية، خدمة Github لتبادل التعليمات البرمجية، لكنها توصي المطورين بتشغيل برمجية تعمل على فحص التعليمات البرمجية بحثاً عن كلمات سر أو مفاتيح خاصة قبل السماح للمطور بنشر ومشاركة التعليمات البرمجية التي يعمل عليها

وأوضح ادوين فوديل بأن هذه الأدوات غالباً ما تولد إيجابيات كاذبة، حيث أنه عثر على معلومات كان ينبغي حذفها موجودة ضمن تعليمات برمجية قامت مجموعة 18F بتحميلها، وأشار إلى أنه ليس هناك بديل عن مراجعة التعليمات البرمجية بشكل بشري قبل تحميلها ونشرها ضمن خدمات مثل Github.