مايكروسوفت تتهم مهاجمين باختراق شبكات الطاقة باستغلال برنامج قديم

الخميس 24 نوفمبر 2022 11:58 م

حذّرت شركة مايكروسوفت (Microsoft) من أن متسللين يستغلون خادم ويب غير نشط لاستهداف المؤسسات في قطاع الطاقة.

ففي تحليل نُشر يوم الثلاثاء الماضي، قال باحثو مايكروسوفت إنهم اكتشفوا برمجية مفتوحة المصدر في خادم الويب "بوا" (Boa)، الذي لا يزال يستخدم على نطاق واسع في مجموعة من أجهزة التوجيه والكاميرات الأمنية، بالإضافة إلى مجموعات تطوير البرامج الشائعة "إس دي كيه إس" (SDKs).

ووجدت مايكروسوفت أثناء التحقيق في اقتحام شبكة كهربائية، أنه على الرغم من انتهاء خدمات البرنامج منذ عام 2005، فإن مهاجمين صينيين استخدموا أجهزة عليها البرمجية القديمة للحصول على موطئ قدم في شبكات التكنولوجيا التشغيلية الحديثة، والتي تستخدم لمراقبة النظم الصناعية والتحكم فيها.

وقالت مايكروسوفت إنها حددت مليون عنصرا لخادم "بوا" منتشر على الإنترنت على مستوى العالم على مدى فترة أسبوع واحد، محذرة من أن هذا العنصر المخترق يشكل "خطرًا في سلسلة التوريد قد يؤثر على ملايين المؤسسات والأجهزة".

مايكروسوفت وجدت أن أحدث هجوم كان اختراق شركة تاتا باور في أكتوبر/تشرين الأول الماضي (رويترز)
وأضافت الشركة أنها لا تزال ترى المهاجمين يحاولون استغلال عيوب بوا، التي تشمل خطأ يعتبر شديد الخطورة في مجال الكشف عن المعلومات السرية، وخللا آخر في الوصول إلى الملفات الخاصة بالنظام.

وقالت مايكروسوفت "يمكن أن تسمح نقاط الضعف المعروفة التي تؤثر على هذه المكونات للمهاجمين بجمع معلومات حول أصول الشبكة قبل بدء الهجمات، والوصول إلى شبكة لم يتم اكتشافها من خلال الحصول على معلومات دخول" ، مضيفة أن هذا يمكن أن يسمح للمهاجمين بالحصول على "تأثير أكبر بكثير" عند بدء الهجوم.

وقالت مايكروسوفت إن أحدث هجوم لاحظته كان اختراق شركة تاتا باور في أكتوبر/تشرين الأول. وأدى هذا الانتهاك إلى قيام مجموعة "هايف رانسموار" (Hive ransomware) بنشر البيانات المسروقة من عملاق الطاقة الهندي، والتي تضمنت معلومات حساسة عن الموظفين ورسومات هندسية وسجلات مالية ومصرفية وسجلات عملاء وبعض المفاتيح الخاصة.

وحذّرت الشركة من أن التخفيف من عيوب بوا أمر صعب بسبب استمرار شعبية خادم الويب المتوقف الآن والطبيعة المعقدة لتركيبته. وتوصي مايكروسوفت المؤسسات ومشغلي الشبكات بتصحيح الأجهزة المعرضة للخطر كلما أمكن ذلك، وتحديد الأجهزة ذات المكونات الضعيفة، وتكوين قواعد كشف لتحديد النشاط الضار.