موجز أسبوعي: اختراقات عبر الأطراف الثالثة، ولوحات معلومات مكشوفة، وثغرة غير مصححة لتجاوز شاشة القفل في ويندوز



يستعرض موجز SecurityWeek اختراقًا عبر مورّد لدى Infoblox، وتسللاً إلى حاسوب Fugaku عبر لوحة معلومات عامة، واختراق بيئة اختبار لدى Rakuten Securities، وثغرة غير مصححة في ويندوز 11.

- أكدت Infoblox أن مهاجمين وصلوا إلى بيانات الشركة عبر مورّد لترحيل البيانات تعرّض للاختراق، وأفادت تقارير بأن الملفات المسروقة شملت لقطات إعدادات NIOS لبعض العملاء.
- علّق معهد Riken تشغيل حاسوب Fugaku بعد أن استخدم طرف خارجي لوحة حالة عامة للدخول إلى شبكة العمليات الداخلية.
- أعلنت Rakuten Securities أن اختراق بيئة اختبار في 11 نوفمبر قد يكون كشف بيانات ملايين الحسابات.
- نشر الباحث Nightmare Eclipse ثغرة FastUnlock غير المصححة في ويندوز 11، وتستغل

Narrator لتجاوز شاشة القفل وتتطلب وصولاً فعليًا للجهاز.

- أوقفت Equinor هجومًا على بعض أنظمتها دون تأثير على الإنتاج، وأبلغت Skagerak Energi عن محاولة اختراق محتملة.

يجمع الموجز الأسبوعي من SecurityWeek عدة حوادث تحمل دروسًا عملية لفرق الأمن والمخاطر. وتشترك ثلاثة منها في فكرة واحدة: التعرّض عبر أصول كثيرًا ما تُعامل على أنها منخفضة المخاطر.

الأطراف الثالثة وبيئات الاختبار ولوحات المعلومات العامة

أكدت Infoblox أن مهاجمين وصلوا إلى بعض معلومات الشركة عبر مورّد خارجي لترحيل البيانات تعرّض للاختراق. وتذكر تقارير إعلامية وردت في الموجز أن المورّد تولى ترحيل SharePoint، وأن الملفات المسروقة شملت لقطات إعدادات NIOS لبعض العملاء إضافة إلى بيانات شخصية لموظفين ومعالين. وتقول الشركة إنه لا دليل على تأثر منتجاتها أو خدماتها السحابية أو تحديثات البرمجيات أو عمليات البناء والإصدار.

وفي اليابان، علّق معهد Riken تشغيل حاسوب Fugaku وقطع الوصول الخارجي. وذكر أن طرفًا خارجيًا استخدم لوحة عامة تعرض حالة تشغيل النظام للدخول إلى شبكة العمليات الداخلية والعبث بعدة خوادم. وقد تكون أسماء ما يصل إلى 4,597 مستخدمًا وبريدهم الإلكتروني ومعرّفاتهم انكشفت.

وأعلنت Rakuten Securities أن مهاجمين وصلوا إلى نظام في بيئة اختبار في 11 نوفمبر. وقد تكون معرّفات الدخول ورموز الفروع لما يصل إلى 11.25 مليون حساب، والبيانات الشخصية والمالية لما يصل إلى 4.47 مليون حساب، انكشفت.

أخبار أخرى جديرة بالانتباه

نشر الباحث Nightmare Eclipse أداة FastUnlock، وهي ثغرة يوم صفر غير مصححة في ويندوز 11. وتستغل قارئ الشاشة Narrator لتجاوز شاشة القفل وتنفيذ شيفرة بصلاحيات حساب شاشة القفل. وتتطلب وصولاً فعليًا للجهاز وحسابًا واحدًا على الأقل مرتبطًا بحساب Microsoft عبر الإنترنت.

وقالت Equinor إنها أوقفت هجومًا على بعض أنظمة تقنية المعلومات اكتشفته في 17 نوفمبر، دون تأثير على الإنتاج ودون مؤشر على سرقة البيانات أو تعديلها. وأبلغت Skagerak Energi بعد يوم عن نشاط قد يكون محاولة اختراق، دون أثر تشغيلي.

تشير هذه الحالات مجتمعة إلى مجالات المراجعة نفسها: وصول الموردين إلى البيانات، وانكشاف أنظمة الاختبار والمراقبة، وضوابط الأجهزة الطرفية المشتركة أو المحمولة.

ما يجب فعله الآن

1. راجع الموردين الذين يحتفظون بنسخ من بياناتكم أو إعداداتكم، وتأكد من التزامات الإبلاغ عن الاختراقات في العقود وإلغاء صلاحيات الوصول بعد انتهاء المشاريع.
2. احصر صفحات الحالة ولوحات المعلومات المتاحة للعموم، وتأكد من عدم وجود مسار منها إلى شبكات العمليات الداخلية.
3. طبّق على بيئات الاختبار ضوابط وصول ومراقبة بمستوى بيئة الإنتاج، وتجنّب وضع بيانات عملاء حقيقية

فيها.

4. تعامل مع لقطات إعدادات الأجهزة المشاركة مع الموردين بوصفها بيانات حساسة، وتأكد من حمايتها وعدم الاحتفاظ بها إلا للحاجة.
5. بالنسبة إلى FastUnlock، قيّد الوصول الفعلي إلى أجهزة ويندوز 11، وتابع إرشادات Microsoft بشأن التصحيح، وانظر في تقييد استخدام Narrator على الأجهزة المشتركة عالية المخاطر.
6. راجع خطط الاستجابة للحوادث فيما يخص إخطار الأطراف الثالثة، بما في ذلك الإبلاغ بموجب نظام حماية البيانات الشخصية (PDPL) عند تأثر بيانات شخصية.