الوكالة الوطنية للأمن السيبراني
National Cyber Security Agency

المبادرة الوطنيّة للسلامة الرقميّة
Digital Safety National Initiative

السلامة الرقمية

العدد الثالث / الخميس 30 ربيع الأول 1446هـ - 3 أكتوبر 2024م

هجمات سيبرانية
على سائقي السيارات عبر رموز QR

شركة Dell
تتعرض للاختراق
مرتين خلال أسبوع واحد

دلال العقيدي
الابتكار والإبداع حاضران في المبادرة الوطنية للسلامة الرقمية

شبكة روبوتات صينية
تتمكن من اختراق 260 ألف جهاز

التصيد الاحتيالي
الخطر الأكبر المرتبط بالذكاء الاصطناعي

المحتويات

الابتكار والإبداع حاضران في المبادرة الوطنية للسلامة الرقمية

يُعدّ الفضاء السيبراني بيئة خصبة للابتكار والإبداع؛ خاصةً أن التطورات في هذا المجال أصبحت متسارعة، ما انسحب بشكلٍ مباشر على أنشطة التوعية السيبرانية، فالإبداع والابتكار يُعزّزان من فاعلية الأدوات التوعوية، ويساعدان بشكل مباشر في تحقيق أهدافها.

وانطلاقاً من هذا الطرح، حرصت الوكالة الوطنية للأمن السيبراني على تكريس ثقافة الإبداع والابتكار في مختلف أنشطة وفعاليات المبادرة الوطنية للسلامة الرقمية.

الإبداع والابتكار في المبادرة يظهران على مستويين؛ الشكل والمضمون، فعلى مستوى الشكل -ويُقصَد به طبيعة الأدوات التوعوية المعتمدة-؛ تم تطوير أدوات توعوية مبتكَرة، تشمل التفاعل المباشر بين المدربين والشرائح المستهدَفة، ومن هذه الأدوات: أنشطة تحليل النماذج؛ من خلال اختيار حالات تصيُّد احتيالي أو جرائم إلكترونية حدثت بالفعل، وتحفيز الجمهور المستهدَف على تحليل سلوك الضحية في هذه الجرائم، وتحديد الخطأ الذي ارتكبه. وهذا النوع من التوعية يُعدّ عالي الفاعلية؛ لكونه يدمج بين التوعية النظرية والتطبيقية.

أما على مستوى الإبداع والابتكار في المضمون، فهو يتعلق بالمحتوى التوعوي المقدَّم في سياق المبادرة، وهنا تحرص الوكالة على تقديم محتوى توعوي بالغ الحداثة، ما يُعزّز من قدرة المستهدَفين على التعرُّف على المخاطر السيبرانية الحديثة، وفي هذا المجال سيتم تقديم محتوى توعوي متعلّق بالذكاء الاصطناعي، لا سيما الذكاء الاصطناعي التوليدي، بما يشمل توعية المستهدَفين بكيفية الاستفادة من منصات الذكاء الاصطناعي التوليدي في الحصول على محتوى توعوي في مجال السلامة الرقمية، مثل Chat GPT وغيرها من المنصات المماثلة. وهذه الحداثة من شأنها تعزيز القيمة التوعوية المضافة التي تقدّمها المبادرة.

"

دلال العقيدي

مدير إدارة التميز السيبراني الوطني

شبكة روبوتات صينية تتمكّن من اختراق 260 ألف جهاز

في أواخر شـــهر ســـبتمبر الماضي، حدث هجوم ســـيبراني واســـع النطـــاق نفَّذته مجموعة قراصنة يُعتقد أن لها صلة بالصين، والذي استهدف أكثر من 260,000 جهاز توجيه SOHO (المخصَّصة للمكاتب الصغيرة والمنازل) وكاميرات IP. استغل هذا الهجوم ثغرات أمنية في هذه الأجهزة، التي تُعدّ عادةً أقـــل أماناً مقارنةً بالبنية التحتية المســـتخدَمة في الشـــركات الكبرى. ويُعدّ هـــذا الهجوم جزءاً من التحديات المتزايدة التي تواجهها أجهزة إنترنت الأشياء (IoT)؛ حيث إن التوسع السريع في اســـتخدام الأجهزة المتصلة بالإنترنت أدى إلى خلق فرص جديدة للمهاجمين السيبرانيين[1].

1. Pernet, Cedric. China-Linked Attack Hits 260,000 Devices. Tech Republic, September 2024, on site: https://www.techrepublic.com/article/china-ddos-attack-fbi-confirms/

هجوم سـيبراني ينجح في تجنيد أجهزة في شـبكة «البوت نت» الكبيرة دون أن يشعر أصحابها بذلك

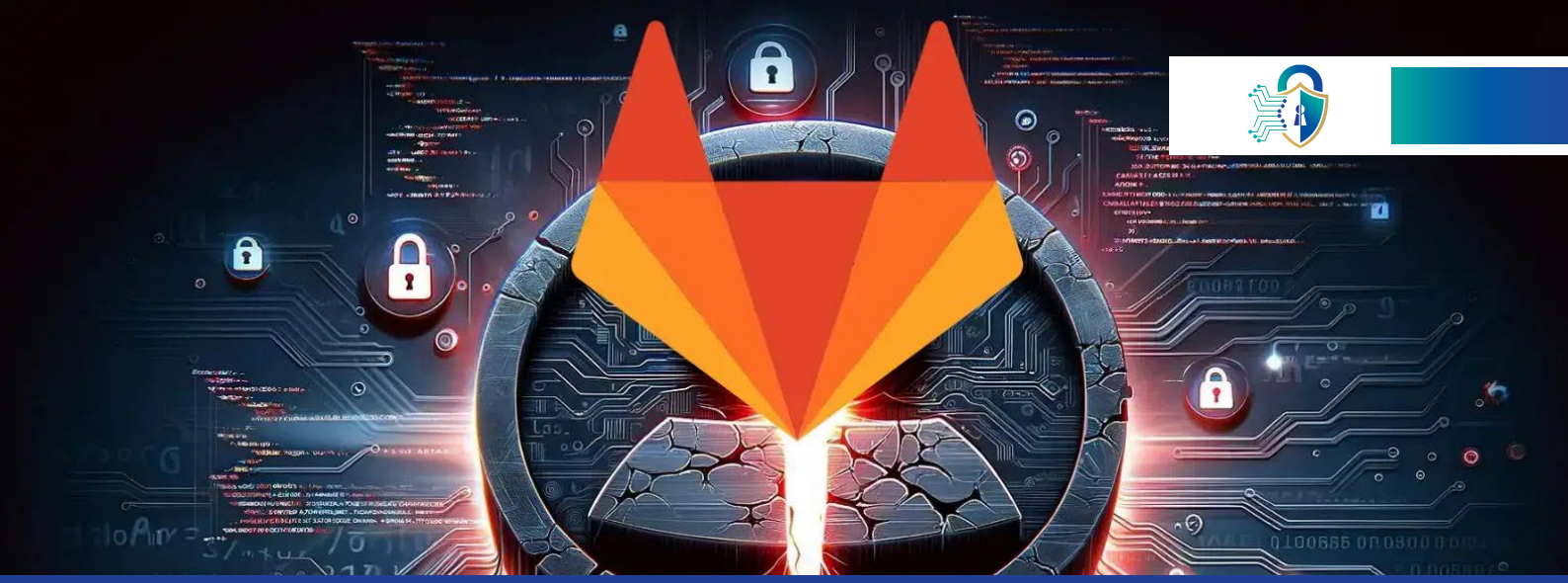
«البوت نت»، وهو مصطلح يشير إلى شبكة ضخمة من الأجهزة التي تم اختراقها واستخدامها بشكل جماعي لشنّ هجمات إلكترونية، يمكن استغلالها في تنفيذ عدة أنواع من الهجمات، مثل هجمات الحرمان من الخدمة (DDoS)، والتجسس على البيانات، وحتى التلاعب بالأجهزة المصابة. في هذه الحالة، تم استهداف أجهزة التوجيه (الراوتر)، وكاميرات IP المستخدَمة بشكلٍ واسع في المنازل والشركات الصغيرة، مما جعل هذه الأجهزة نقاط دخول مثالية للمهاجمين. وغالباً ما تكون هذه الأجهزة غير محدَّثة، أو تم إعدادها باستخدام إعدادات افتراضية غير آمِنَة، ما يُتيح للمهاجمين سهولة الوصول إليها[1].

وفي هذا الشأن تشير التقارير إلى أن القراصنة قاموا بتجنيد هذه الأجهزة في شبكة «البوت نت» الكبيرة دون أن يشعر أصحاب الأجهزة بذلك. وتمّت برمجة «البوت نت» لتكون متحكّمة بالأجهزة المصابة؛ حيث يمكن للقراصنة إصدار أوامر لهذه الأجهزة لتنفيذ عمليات تخريبية عن بُعْد. مثل هذه الهجمات لا تُؤثِّر فقط على الأجهزة المصابة بشكلٍ مباشر، بل يمكن استخدامها في شنّ هجمات على نطاق أوسع؛ مثل الهجمات على خوادم شركات كبيرة، أو استخدام «البوت نت» لتوليد حركة مرور ضخمة لتعطيل خدمات الويب.

أحد أبرز التحديات التي تَفرضها مثل هذه الهجمات هو ضعف القدرة على اكتشاف الأجهزة المصابة. في كثير من الحالات، لا يُدْرك أصحاب أجهزة التوجيه أو الكاميرات أن أجهزتهم قد تم اختراقها؛ حيث لا تظهر علامات واضحة على وجود خلل. حتى عندما يتم اكتشاف المشكلة، قد يكون الأوان قد فات لإصلاح الأضرار أو منع استخدامها في هجمات مستقبلية. وتشير هذه الحوادث إلى الحاجة المُلِحَّة لتعزيز الوعي الأمني بين مستخدمي الأجهزة المتصلة بالإنترنت، سواء في المنازل أو في الشركات الصغيرة، وتحديث الأجهزة بانتظام واستخدام كلمات مرور قوية وغير افتراضية.

الهجوم الأخير يعكس أيضاً مدى تعقيد التهديدات السيبرانية الحديثة والتطور السريع في أساليب الاختراق. فلم تَعُد الهجمات السيبرانية مقتصرةً على الشركات الكبرى أو الحكومات، بل أصبحت تطال الأفراد والمؤسسات الصغيرة بشكل متزايد. مع تزايد الاعتماد على الأجهزة المتصلة، يصبح من الضروري تعزيز الجهود العالمية لتحسين أمن هذه الأجهزة وتطوير إستراتيجيات أكثر فاعلية لحمايتها.

1. Ilascu, Ionut. Chinese botnet infects 260,000 SOHO routers, IP cameras with malware, Bleepingcomputer, September 2024, on site: https://www.bleepingcomputer.com/news/security/flax-typhoon-hackers-infect-260-000-routers-ip-cameras-with-botnet-malware/



منصة GitLab
تُصدر تصحيحاً أمنياً مهماً يعالج 17 ثغرة أمنية

أصــدرت GitLab تحديثــاً أمنياً مهماً يُعالــج العديد من الثغرات الأمنية الحرجة، ممــا جعل هذا التحديث موضع اهتمام واسع في مجتمع الأمن السيبراني.

جديــر بالذكر أن منصة GitLab تُعدّ واحدة من أشــهر المنصات المســتخدَمة لإدارة وتطوير المشــاريع البرمجية، وتحظى بشعبية كبيرة بين المطوّرين والشركات على مستوى العالم. ومع هذه الشهرة الكبيرة تتزايد فرص التهديدات بالهجمات السيبرانية التي تَستهدف استغلال أيّ ثغرات موجودة في النظام.

منصــة GitLab تكتشــف ثغــرات أمنية في نظامها وتُصــدر تحديثاً لمعالجتها

جــاء التحديث الأخير اســتجابةً لعدد مــن الثغرات المكتَشــفة في نظام GitLab، التي بلغ عددها 17 ثغرة، تتــراوح بين ثغرات متوســطة وحرجة. إحدى الثغــرات الأكثــر خطورة كانت تســمح للمهاجمين بتنفيــذ تعليمات برمجيــة عن بُعْد علــى الخوادم المتأثرة، مما يُتيح لهم السيطرة على النظام بشكل كامل. ويتم تصنيف هــذه الأنواع من الثغرات على أنها مــن أخطر أنــواع الهجمات الســيبرانية؛ لأنها تُتيــح للمهاجمين الوصول إلى الخــوادم والبيانات الحساســة دون الحاجة إلى الوجود الفعلي بالقرب من الهدف.

وفقاً للتفاصيل التي تم إصدارها؛ فإن هذا التحديث شــمل إصلاحات لعدد من المشــكلات المتعلقة بــإدارة الأذونات والتصديق داخــل النظام، وهو ما يُمثّل نقطة ضعف كبيرة إذا ما تم استغلالها.

وكانت بعض هذه الثغرات تُتيح للمســتخدمين غير المصرَّح لهم إمكانية الوصول إلى بيانات أو عمليات لا يجب أن يكون لهــم صلاحية الوصول إليها. وهذا ما جعل GitLab تســارع لإصدار التحديثات لتصحيح هذه الأوضاع وتجنُّب أيّ استغلال محتمَل مِن قِبَل المهاجمين.

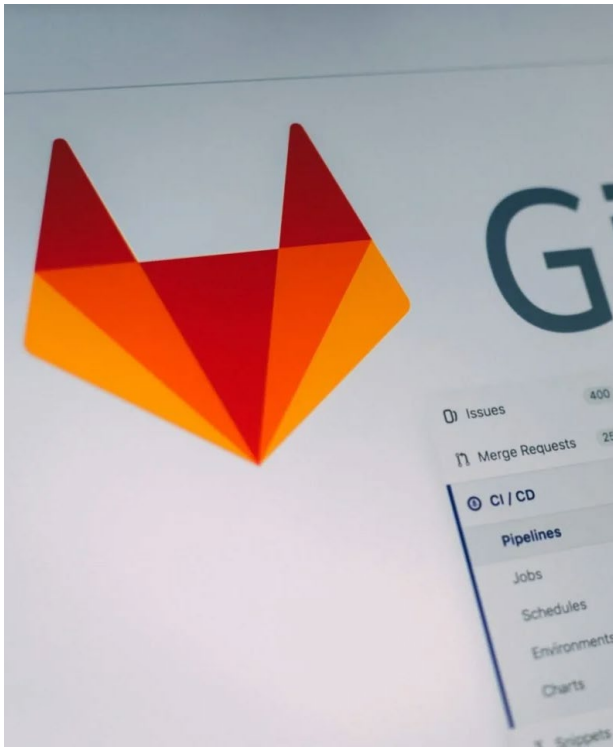
اكتشـــاف ثغرة أمنية حَرِجة في منصة GitLab تســـمح للمهاجمين بتنفيذ تعليمات برمجية عن بُعْد على الخوادم المتأثرة، مما يُتيح لهم الســـيطرة على النظام بشكل كامل

جـــاء هذا التحديث فـــي وقتٍ حرج بالنســـبة للكثير من الشـــركات التي تعتمد بشكل كبير على GitLab لإدارة مشـــاريعها وتطويـــر برمجياتها. فعلى الرغم من أن GitLab قد اكتســـبت سُمعة قوية من حيث أمانها واستقرارها؛ إلا أن اكتشاف مثل هذه الثغرات يُعيـــد التأكيد على الحاجـــة الدائمة إلـــى المتابعة المســـتمرة والتحديثات الأمنية الســـريعة. وأكَّدت GitLab في بيانها أن جميع المســـتخدِمين يجب أن يقوموا بتحديث أنظمتهم في أســـرع وقتٍ لضمان حمايتها من أيّ استغلال محتمَل[1].

جديـــر بالذكـــر أن GitLab تعمل بشـــكل دائم على تعزيز أمـــان منصتها من خلال التعـــاون مع مجتمع المطوّريـــن والباحثيـــن الأمنييـــن. هـــذه العلاقة التعاونيـــة تســـمح بالكشـــف عن الثغرات بســـرعة وتقديم الحلول المناســـبة لها. كما تعتمد الشركة على برنامج المكافآت للكشـــف عن الثغرات (bug bounty)، الـــذي يشـــجّع الباحثيـــن الأمنيين على الإبلاغ عـــن أيّ مشـــكلات أمنية قد يكتشـــفونها مقابل مكافآت مالية.

في ظـــل التطورات المتســـارعة فـــي مجال الأمن السيبراني وتزايد الهجمات التي تستهدف المنصات التكنولوجيـــة الكبرى، تصبح التحديثات الأمنية جزءاً أساســـياً من دورة حياة أيّ نظام برمجي. ويُعدّ هذا التحديـــث من GitLab مثـــالاً واضحـــاً على أهمية الاســـتجابة الســـريعة للتهديدات الأمنية وكيفية التكيُّـــف معها. كما يُبـــرز ضرورة الالتـــزام بتطبيق التحديثـــات الأمنية بانتظام للحفـــاظ على سلامة النظام وبيانات المستخدمين.

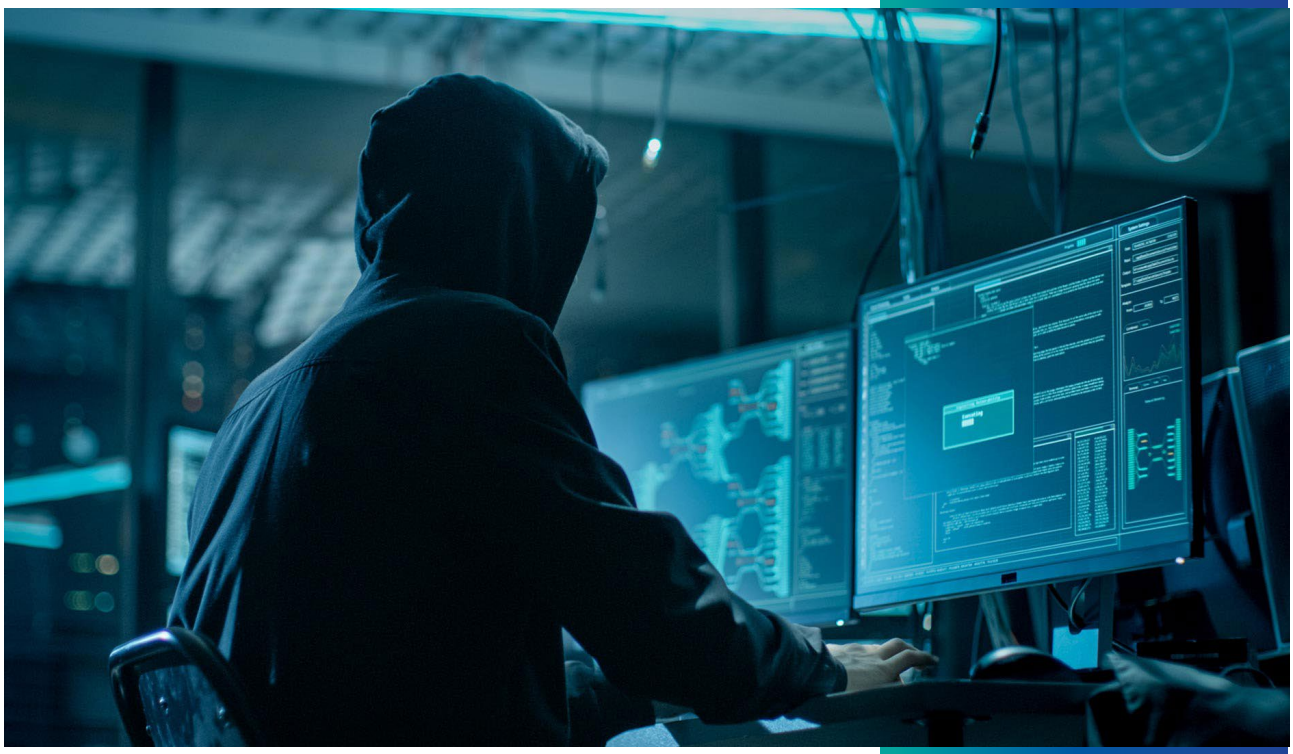
في النهاية، يُظهر هذا التحديث أن GitLab تأخذ أمن منصتها على محمل الجد، وتسعى دائماً إلى تحسين مستوى الحماية لتأمين مشاريع المستخدمين من أيّ تهديدات ســـيبرانية قد تواجههـــم. ومع ذلك، يجب على المســـتخدِمين أن يدركوا أن الأمان ليس مســـؤولية الشـــركة وحدها، بل يجب أن يكون جزءاً من ثقافة كلّ منظمة ومطوّر.



1. Alger, Jordyn. GitLab releases security updates to fix 17 vulnerabilities, Security Magazine, September 2024, on site: https://2u.pw/YLyK8FTO

التصيد الاحتيالي

الخطر الأكبر المرتبط بالذكاء الاصطناعي



أصبح الذكاء الاصطناعي (AI) قوة دافعة في تعزيز الأمن السيبراني. بفضل قدرته على تحليل كميات هائلة من البيانات وتعلُّم الأنماط السلوكية المعقَّدة، يساعد الذكاء الاصطناعي في اكتشاف التهديدات السيبرانية بشكل أسرع وأكثر دقة. ومع ذلك، لا يأمن الذكاء الاصطناعي من التحديات الأمنية؛ إذ كشفت تقارير حديثة أن 75% من المنظمات تَعتبر التصيد الاحتيالي (Phishing) هو أكبر خطر مرتبط بالذكاء الاصطناعي[1].

1. 75% of organizations say phishing poses the greatest AI risk, , Security Magazine, September 2024, on site: https://2u.pw/B9eAssnV

الذكاء الاصطناعي سلاح ذو حدين.. انتشـــار رسائل بريد إلكتروني تصيدية مصمَّمة بالذكاء الاصطناعي تبدو واقعية تماماً

التصيُّد الاحتيالي، الذي يعتمـــد على خداع الأفراد للكشـــف عن معلوماتهم الحساســـة مثل كلمات المـــرور أو البيانات المالية، شـــهد تطـــوراً هائلاً مع دخول الذكاء الاصطناعي إلى هذا المجال. القراصنة يســـتخدمون تقنيات الـــذكاء الاصطناعي لتصميم رســـائل بريد إلكتروني ورســـائل نصية تبدو واقعية تماماً، مما يجعل من الصعـــب على الضحايا التمييز بين الرسائل الحقيقية والمزيفة. الذكاء الاصطناعي يسمح أيضاً بتحليل الأنماط السلوكية للمستخدمين، مما يُمكّن المهاجمين من توجيه الهجمات بشـــكل أكثر دقـــة وفاعلية، واســـتهداف الأفراد الذين من المحتمَل أن يستجيبوا لتلك الهجمات.

ويُســـتخدم الـــذكاء الاصطناعي أيضاً فـــي التصيد الاحتيالـــي عبـــر تقنيـــات التعلم الآلي التـــي تُمكّن القراصنـــة مـــن تحليـــل رســـائل البريـــد الإلكتروني المرسَلة من الشـــركات، ومحاكاة اللغة والأسلوب المســـتخدَمَيْن في هذه الرســـائل. ويمكن للذكاء الاصطناعـــي توليد رســـائل احتياليـــة تحمل توقيع الشركة الحقيقي، وتبدو كما لو أنها تأتي من جهات رســـمية، مثل البنوك أو الجهـــات الحكومية. وهذا يجعل من الصعب للغاية اكتشـــاف هذه الهجمات بالوسائل التقليدية.

75% من الشـــركات تعتبر التصيد الاحتيالـــي (Phishing) هو أكبر خطر مرتبط بالذكاء الاصطناعي

ورغم هذه المخاطر، فإن الذكاء الاصطناعي يمكن أن يكـــون سلاحاً فعّـــالاً ضد التصيـــد الاحتيالي إذا تم اســـتخدامه بطريقة صحيحة. ويستخدم العديد مـــن مقدّمي خدمـــات الأمـــن الســـيبراني الذكاء الاصطناعي لتحليل ســـلوكيات البريـــد الإلكتروني والأنمـــاط الرقميـــة للمســـتخدِمين؛ لاكتشـــاف الأنشطة المشبوهة في الوقت الحقيقي؛ حيث إن أنظمة الـــذكاء الاصطناعي قادرة على تحليل مئات الآلاف من الرسائل الإلكترونية في لحظات، وتحديد الرســـائل التي تحتوي على تهديدات محتملة، مثل الروابط الضارة أو المرفقات المشبوهة.

ومـــع ذلـــك، يبـــدو أن هنـــاك فجـــوة كبيـــرة بين التهديـــدات التـــي تُشـــكّلها الهجمات المســـتندة إلى الـــذكاء الاصطناعي والإجـــراءات التي تتَّخذها الشـــركات للحماية منها؛ فقد كشف تقرير صادر عن إحدى الشـــركات العالمية أن 75% من المؤسسات تعتـــرف بخطر التصيـــد الاحتيالي الناتـــج عن الذكاء الاصطناعـــي، ومع ذلـــك لا تزال العديـــد منها غير مجهَّزة بالكامل للتعامل مع هذه الأنواع المتطورة مـــن الهجمات. وهـــذا يعكس الحاجـــة الملحَّة إلى تعزيز تقنيـــات الحماية وتطوير الأدوات التي تعتمد على الذكاء الاصطناعي للكشـــف عـــن التهديدات والتصدي لها.

إلى جانب التصيد الاحتيالي، يمكن استخدام الذكاء الاصطناعي في أشكال أخرى من الجرائم الإلكترونية، مثل هجمات الروبوتات (botnets)، وهجمات الحرمان من الخدمة (DDoS). لكن في المقابل، يسهم الذكاء الاصطناعي في تحسين أنظمة الدفاع السيبراني بفضل قدرته على اكتشاف التهديدات غير المعروفة وتقديم استجابات سريعة.

في النهاية، فإن الذكاء الاصطناعي يُعدّ سلاحاً ذا حدين في مجال الأمن السيبراني، فبينما يستخدم القراصنة هذه التكنولوجيا لشنّ هجمات متطورة، يمكن في المقابل توظيفها لبناء أنظمة دفاع قوية. ويتعين على المنظمات أن تستثمر بشكلٍ أكبر في الذكاء الاصطناعي كأداة للكشف عن التهديدات، وتطوير إستراتيجيات للتعامل مع التهديدات السيبرانية التي تعتمد على الذكاء الاصطناعي.

«هجمات سيبرانية»

على سائقي السيارات عبر رموز QR

شـهدت المملكة المتحـدة ارتفاعـاً ملحوظاً في عمليات الاحتيال عبر رموز QR، مسـتهدفةً سائقي السـيارات. وهـذا النـوع مـن الهجمات يسـتغل التكنولوجيـا الشـائعة المسـتخدَمة فـي الحياة اليوميـة؛ حيث يعتمـد المهاجمون على تسـهيل عملية مسح رموز QR لسرقة المعلومات الشخصية والمالية للسـائقين. رموز QR، التي تُستخدم عادةً للدفع الإلكتروني أو الوصول إلى معلومات محدَّدة، أصبحت وسيلة استهداف فعَّالة للمحتالين؛ وذلك بفضل السرعة وسهولة الاستخدام.

هجمـات عبـر رمـوز QR تعتمد على اسـتغلال ثقة المستخدمين بالتكنولوجيا

يتمثل السـيناريو الأكثر شيوعاً لهذه الهجمات في أن المهاجمين يضعون رمـوز QR مزيفة في أماكن متعددة، مثل أجهزة الدفع في مواقف السـيارات، أو حتى يلصقونها فوق الرموز الأصلية. عندما يقوم السائقون بمسـح هذه الرموز باستخدام هواتفهم الذكية، يتـم توجيههم إلى مواقع إلكترونية مزيَّفة تشـبه المواقـع الرسـمية، ولكنهـا تهـدف إلى سرقة معلوماتهم الشـخصية أو بيانات بطاقاتهم الائتمانية. بعض هذه المواقع المزيفة تحتوي على

نماذج لتعبئة بيانات حساسة مثل الأرقام السرية أو تفاصيل الحسابات البنكية.

وتُعـدّ الهجمات عبر رموز QR خَطرة بشـكلٍ خاص؛ لأنهـا تعتمـد على اسـتغلال ثقة المسـتخدمين بالتكنولوجيا؛ حيث يُعتبر مسح رمز QR إجراءً بسيطاً ولا يتطلـب التفكير الكثير، مما يجعـل الناس أقل حذراً عند اسـتخدامه مقارنةً بطـرق الدفع الأخرى التي تتطلب خطـوات إضافية أو طبقات أمان مثل التحقق بخطوتين. وبالتالي، يسهل على المهاجمين اسـتهداف مجموعة كبيرة مـن الضحايا في وقت قصير.

ووفقاً للتقارير؛ فقد ارتفعـت العمليات الاحتيالية في مواقف السيارات العامة؛ حيث يجد السائقون رمـوز QR مزيفـة تحـلّ مـكان الرموز الشـرعية، ويقومـون بإدخـال معلوماتهـم دون وعـي بأن

الموقع الذي وصلوا إليه غير آمِن. عمليات الاحتيال هــذه لا تُؤثّر فقط على الســائقين الأفــراد، ولكن أيضاً على الشركات والمؤسسات التي تعتمد على هذه التكنولوجيا لتســهيل الدفع والخدمات. وقد تجد هذه الشــركات نفســها في مواجهة شكاوى متعــددة من العملاء حــول اختراق حســاباتهم أو سرقة أموالهم.

عمليــات احتيــال واســعة النطاق باســتخدام رموز QR لسرقة المعلومات الشخصية والمالية للسائقين

واســتجابةً لهــذه التهديدات؛ أصدرت الســلطات البريطانيــة تحذيرات للســائقين والجمهــور العام بضرورة توخّي الحذر عند مســح رمــوز QR . ونُصِحَ السائقون بالتأكد من أن الموقع الذي يتم توجيههم إليه بعد المســح هو موقع رسمي ومعروف، وألا يقوموا بإدخال أيّ معلومات شــخصية أو مالية إذا شــعروا بأن الموقع غير مألــوف، أو إذا لاحظوا أيّ شــيء مريب. بالإضافة إلى ذلك، تشــجع الهيئات الأمنية على اســتخدام برامج حمايــة الهاتف مثل التطبيقــات التي تكتشــف الروابط المشــبوهة أو تحذر من المواقع غير الآمنة[1]. أيضاً، تحثّ الشركات التي تعتمد علــى رموز QR لتحصيل المدفوعات أو تقديــم خدماتها على اتخاذ تدابيــر إضافية لضمان أمــان هذه الرمــوز. على ســبيل المثــال، يمكنهم طباعة الرموز بشــكل مباشــر على مواد غير قابلة للتغيير أو اســتخدام تقنيــات حماية مثل العلامات المائية الرقمية لمنع تزوير الرموز.

في الختــام، تُعدّ عمليــات الاحتيال عبــر رموز QR تهديــداً حديثاً يعكــس كيف يســتغل المهاجمون أيّ ثغــرة في التكنولوجيــا للوصول إلــى الضحايا. علــى الرغم مــن أن رموز QR تُســتخدَم لتســهيل المعاملات الرقميــة؛ إلا أن الاعتماد المفرط عليها دون اتخــاذ تدابير أمان كافيــة يمكن أن يفتح الباب أمام استغلالها. ويحتاج السائقون والمستخدمون في أنحاء العالم إلى توخّي الحذر عند استخدام هذه التقنية لضمان حماية بياناتهم الشخصية والمالية.

1. Osborne, Hilary. UK motorists warned of fake parking QR codes being used in ‘quishing’ scams, The Guardian, august 2024, on site: https://2u.pw/xhQaOQXR

شركة Dell

تتعرَّض للاختراق مرتين خلال أسبوع واحد

تعرَّضت شـــركة Dell، وهي واحدة من أكبر الشـــركات في مجال التكنولوجيا وتصنيع أجهزة الحاســـوب، لهجومين سيبرانيين كبيرين في غضون أسبوع واحد. هذه الاختراقات أثارت ضجة كبيرة في أوساط الأمن السيبراني؛ حيث تمت الإشارة إلى أن المهاجمين استغلوا ثغرات في النظام للوصول إلى بيانات حساسة داخلية، مما يعكس خطورة الهجمات السيبرانية المستمرة التي تستهدف الشركات الكبرى.

ثغرات أمنية في أنظمة Dell تتسبَّب باختراق الشركة مرتين خلال أسبوع واحد

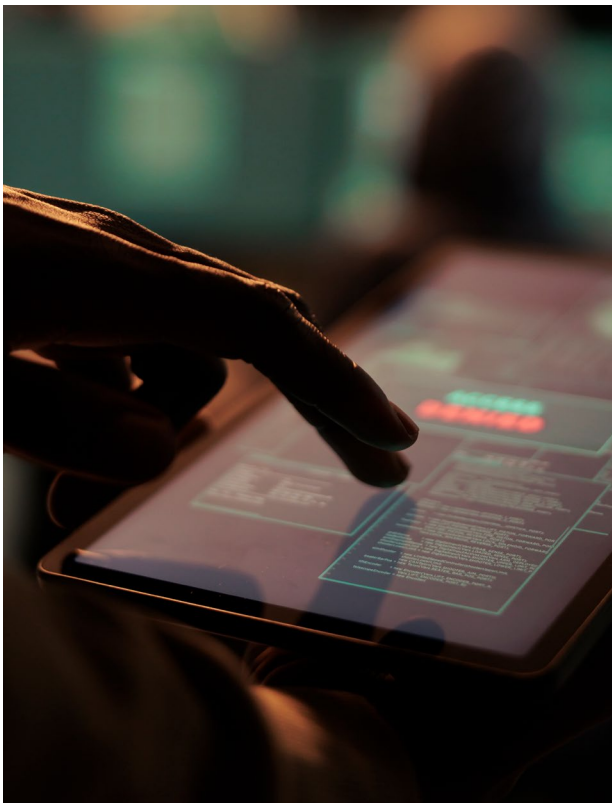
بدأ الهجوم الأول عندما استغل قراصنة سيبرانيون ثغرات أمنية في أنظمة Dell، وتمكنوا من الوصول إلى بيانات داخلية حساسة. ورغم عدم توفّر تفاصيل دقيقة حول كيفية وصول القراصنة إلى هذه البيانات؛ إلا أن التقارير تشير إلى أن الهجوم استهدَف أحد البرامج المستخدَمة على نطاق واسع في الشركة، وهو برنامج Atlassian. استغل المهاجمون ثغرة غير مكتشفة في هذا البرنامج للتمكُّن من التسلل إلى أنظمة الشركة. وهذا النوع من الهجمات معروف باسم "هجوم استغلال الثغرات يوم الصفر" (zero-day exploit)؛ حيث يتم استغلال ثغرات في البرامج التي لم يتم الكشف عنها بعد، أو لم يتم إصلاحها مِن قِبَل الشركات المطورة[1].

لم يكد فريق الأمن السيبراني في Dell يبدأ في التعامل مع هذا الاختراق حتى تعرَّضت الشركة لهجوم ثانٍ بعد بضعة أيام. في هذه المرة، استخدم القراصنة تقنيات جديدة للوصول إلى الأنظمة الداخلية، مما جعل عملية التحقيق والتعامل مع الهجمات أكثر تعقيداً. وعلى الرغم من عدم الإعلان عن تفاصيل دقيقة حول الهجوم الثاني؛ إلا أن شركة Dell أكدت أنها كانت ضحية لعملية سيبرانية متطوّرة تهدف إلى استغلال الأنظمة والبنية التحتية الرقمية الخاصة بها. ويُعتقَد أن المهاجمين كانوا يستهدفون ملفات حساسة تتعلق بعمليات الشركة، وربما بيانات العملاء، مما يشكّل تهديداً جدياً للأمان السيبراني.

1. Sharma, Shweta. Hacker selling Dell employees' data after a second alleged data breach, Csoonline, September 2024, on site: https://www.csoonline.com/article/3536783/hacker-selling-dell-employees-data-after-a-second-alleged-data-breach.html

ثغرات في نظام شركة Dell تُمكّن مهاجمين سيبرانيين من الوصول إلى بيانات حساسة داخلية

أثار الهجومان قلقاً كبيراً ليس فقط داخل Dell، ولكن أيضاً في مجتمع الأمن السيبراني بشكل عام. إذ يعكس الهجومان تطوُّر التهديدات السيبرانية وقدرة القراصنة على استغلال نقاط الضعف في الأنظمة الكبرى. وإن شركة بحجم Dell، التي تعتمد على بنية تحتية تقنية قوية، وتستثمر بكثافة في الأمن السيبراني، تُظهر من خلال هذه الحادثة أنه حتى أقوى الشركات ليست محصَّنة ضد هذه الهجمات[1].



في ظل هذه الأحداث، قامت Dell باتخاذ إجراءات فورية لتعزيز أنظمتها الأمنية؛ حيث تم البدء في تحقيق داخلي بالتعاون مع فِرَق من خبراء الأمن السيبراني، إلى جانب استدعاء شركات خارجية متخصصة للتحقيق في كيفية وقوع الهجمات وتحديد الثغرات التي تم استغلالها. كما أصدرت Dell بياناً علنياً دعت فيه عملاءها وشركاءها إلى اليقظة واتخاذ الإجراءات اللازمة لحماية أنظمتهم.

1. Croft, Daniel. Dell allegedly breached twice in 1 weekend, Cyber Daily, September 2024, on site: https://www.cyberdaily.au/security/11141-dell-allegedly-breached-twice-in-one-weekend

الهجمـــات المتكررة علـــى Dell خلال فتـــرة زمنية قصيرة؛ تؤكد على أهمية التطوير المســـتمر لحلول الأمن الســـيبراني، والتحديث الدائـــم للبنية التحتية الرقميـــة. ففي عالـــمٍ يتزايـــد فيه الاعتمـــاد على التكنولوجيا والاتصال عبر الإنترنت؛ تُصبح الشركات الكبرى هدفاً مغرياً للقراصنة، ســـواء بدافع السرقة المالية أو التجســـس الصناعي. وحالـــة Dell تمثّل جرس إنذار للشـــركات العالمية لتعزيز إستراتيجيات الأمان، والتأكد مـــن تأمين جميع الثغرات الممكنة، حتى في البرامج التي تبدو غير مهمة.

هـــذه الحـــوادث تُســـلّط الضـــوء علـــى التحديات المتزايدة التي تُواجه الشركات الكبرى في مواجهة التهديدات الســـيبرانية. وبينما يمكن لشركات مثل Dell أن تتعافى بســـرعة بسبب استثماراتها الكبيرة في التكنولوجيا؛ فإن العديد من الشـــركات الأخرى قد لا تملك نفس الحظ.

اكتشاف ثغرة خطيرة في أنظمة Nvidia

ثغــرة أمنية في أنظمة Nvidia تُمكّن المهاجمين من الوصول غير المصرَّح به إلى الجهاز والتحكم فيه بشكل كامل

كشــفت تقارير أمنية عن ثغرة خطيرة في أنظمة Nvidia، الشــركة الرائدة فــي صناعة وحدات معالجة الرسومات (GPU) والبرمجيات المرتبطة بها. هذه الثغرة، التي تم تصنيفها على أنها عالية الخطورة، تُهدّد الملايين من المستخدِمين حول العالم؛ إذ يمكن استغلالها لتنفيذ هجمات عن بُعْد والتحكُّم في الأنظمة التي تعمل بوحدات Nvidia.

الثغرة المكتشفة تتعلق بوحدات معالجة الرسومات من سلســلة GeForce & RTX، التــي تعتمد على برنامج تشــغيل Nvidia Display Driver. وتكمن المشــكلة في آليــة التعامل مع البيانــات التي تمر عبر هذه الوحدات؛ حيث يمكن للمهاجمين عن بُعْد استغلال الثغرة لتنفيذ تعليمات ضارَّة على النظام، ما يســمح لهم بالوصول غير المصرح به إلى الجهاز والتحكم فيه بشكل كامل. هذا النوع من الهجمات يُعرف باســم "هجوم تنفيذ التعليمات البرمجية عن بُعــد" (Remote Code Execution - RCE)، وهو من أخطر أنواع الهجمات الســيبرانية؛ لأنه يســمح للمهاجميــن بالتلاعــب بالنظــام دون الحاجة إلى الاتصال المباشر بالجهاز المستهدَف[1].

وفقــاً للتقارير، يمكن اســتغلال الثغرة عبر إرســال بيانات ضــارة إلى برنامج التشــغيل، مما يؤدي إلى تعطيل حماية النظام، وتنفيذ الهجوم. وتشمل الآثار المحتملة لهذه الثغرة ســرقة البيانات الحساســة، مثل المعلومات الشخصية أو المالية، بالإضافة إلى إمكانية استخدام الأجهزة المصابة لتنفيذ هجمات

1. Tamar, Shir. et al, Vulnerability Affecting Containers Using NVIDIA GPUs, Wiz, , September 2024, on site: https://www.wiz.io/blog/wiz-research-critical-nvidia-ai-vulnerability

أخرى، مثل هجمات الحرمان من الخدمة (DDoS)، أو استخدام موارد الجهاز في عمليات تعدين العملات الرقمية بشكل غير قانوني.

شركة Nvidia سارعت فور اكتشاف الثغرة إلى إصدار تحديث أمني لمعالجة هذه المشكلة، داعيةً المستخدمين إلى تحديث برامج التشغيل الخاصة بهم فوراً؛ لتجنُّب استغلال الثغرة مِن قِبَل المهاجمين. يأتي هذا التحديث كجزء من الجهود المستمرَّة لتعزيز أمان منتجاتها وحماية مستخدميها من التهديدات السيبرانية المتزايدة. التحديث شمل إصلاحات متعددة للثغرات المكتشَفة، بما في ذلك الثغرة الحَرِجة التي تمّ تحديدها برمز CVE-2024-1234، وهو الترميز الذي يُستخدَم لتصنيف الثغرات الأمنية بحسب درجة خطورتها وانتشارها[1].

ما يزيد من خطورة هذه الثغرة هو الانتشار الواسع لوحدات معالجة Nvidia في مختلف المجالات، من الألعاب إلى التطبيقات الصناعية والتجارية. ومع اعتماد ملايين المستخدمين على هذه الوحدات لتشغيل أنظمتهم؛ تصبح الثغرة فرصة مغرية للمهاجمين لاستغلالها على نطاق واسع.

كما تتزايد مخاطر الهجمات السيبرانية عندما يتعلق الأمر بالأجهزة المتصلة بالإنترنت، أو تلك التي تُستخدم في البنية التحتية الحيوية؛ مما يجعل التعامل مع هذه الثغرة أمراً بالغ الأهمية.

1. Naraine, Ryan. Critical Nvidia Security Flaw Exposes Cloud AI Systems to Host Takeover, Security Week, , September 2024, on site: https://www.securityweek.com/critical-nvidia-container-flaw-exposes-cloud-ai-systems-to-host-takeover/

بينما تمكّنت Nvidia من التعامل بسرعةٍ مع هذا التهديد؛ عبر إصدار التحديثات اللازمة، يبقى السؤال حول مدى استعداد المستخدمين لتطبيق هذه التحديثات في الوقت المناسب؛ حيث إن تأخير تحديث برامج التشغيل يمكن أن يُتيح للمهاجمين استغلال الثغرة، وإلحاق الضرر بالأنظمة قبل أن يتم تأمينها بشكل كامل.

وتُعدّ هذه الحادثة تذكيراً واضحاً بأهمية التحديثات الأمنية المستمرة، والحفاظ على الأنظمة مُحدَّثة بأحدث الإصدارات من البرامج. وفي ظل التطور السريع للتكنولوجيا وازدياد اعتماد الأنظمة على وحدات المعالجة المتصلة، تصبح التهديدات السيبرانية أكثر تعقيداً وخطورة. الثغرات مثل تلك التي اكتُشِفَت في أنظمة Nvidia تُؤكّد على الحاجة الدائمة لتعزيز الحماية السيبرانية، سواء مِن قِبَل الشركات المُصنّعة أو المستخدمين أنفسهم.

بينما تستمر Nvidia في تعزيز أمان منتجاتها، تبقى هذه الحادثة مثالاً على مدى خطورة الثغرات الأمنية في الأجهزة الرقمية المتقدّمة. ويتطلب ذلك من المستخدمين والمطورين التزاماً مستمراً بالحماية والتحديثات للتصدّي لهذه التهديدات المتطورة بشكلٍ فعّال.

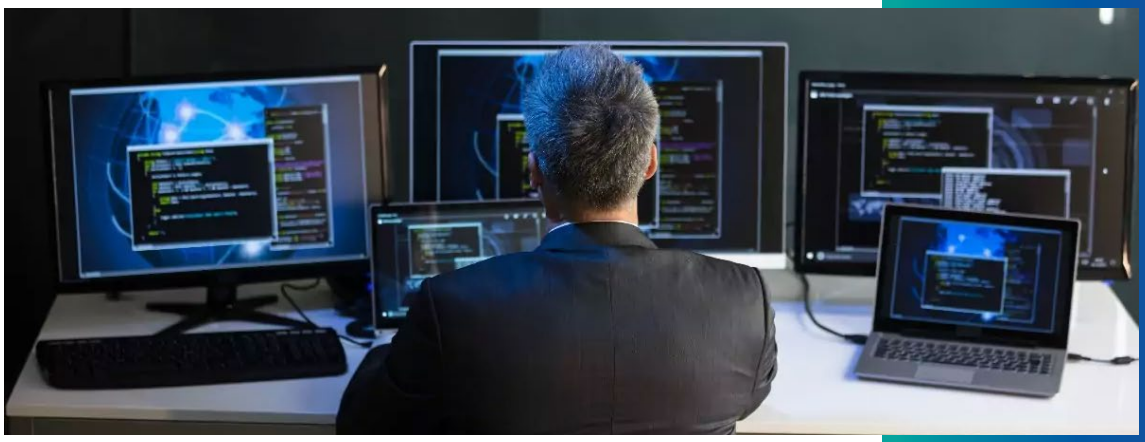
ثغرة في Linux

تؤدي إلى تنفيذ التعليمات البرمجية عن بُعْد

مؤخــراً أظهــرت تقارير أمنية وجــود ثغرة خطيرة في نظام التشــغيل Linux يمكن أن تــؤدي إلى تنفيذ التعليمــات البرمجية عن بُعْــد (Remote Code Execution - RCE). هذه الثغرة، التي وُصفت بأنها عالية الخطورة، أثارت قلقاً كبيراً في الأوساط السيبرانية؛ نظراً لأن نظام Linux يُستخدَم على نطاق واسع في العديد من المجالات، بدءاً من الخوادم الكبيرة وحتى الأجهزة الشخصية والأنظمة المدمجة.

تتعلق الثغرة بآلية معالجة معينة في نواة نظام التشغيل Linux، وهي القلب الأساســي للنظام الذي يتحكم فــي جميع العمليات التي تُجرى داخل النظام. من خلال اســتغلال هذه الثغرة، يمكن للمهاجمين إرسال

ثغــرة خطيــرة فــي نظــام التشــغيل Linux تُمكّن المهاجمين من إرسال تعليمات ضارَّة إلى النظام



تعليمات ضــارة إلى النظام مــن بُعْد، وتنفيذها علــى الجهاز المصاب، مما يُتيح لهم إمكانية الســيطرة الكاملة علــى النظام. وهذا النوع من الهجمات يُعتبر خطيراً بشــكلٍ خاصّ؛ لأن المهاجم لا يحتاج إلى الوصول المباشــر إلى الجهاز المســتهدَف، بل يمكنه اســتغلال هذه الثغرة عبر الإنترنت، ما يَفتح الباب أمام احتمالات هجمات واسعة النطاق[1].

1. Bradley, Nick. FYSA – Critical RCE Flaw in GNU-Linux Systems, Security Intelligence, September 2024, on site: https://securityintelligence.com/news/fysa-critical-rce-flaw-in-gnu-linux-systems/

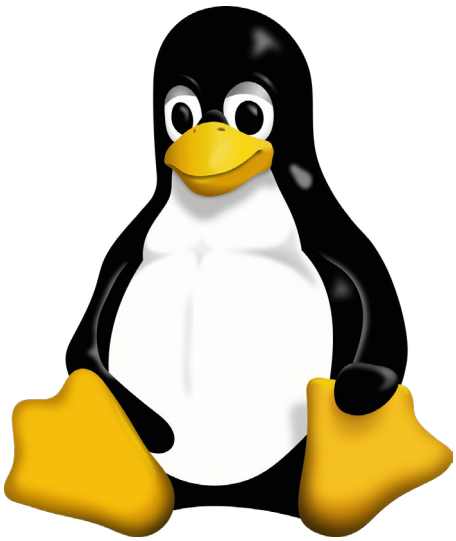
الثغرة المكتشَـفة تحمل رقم CVE-2024-XXXX، وتم تصنيفهـا ضمن الثغرات الحرجـة التي تتطلب إصلاحـاً فوريـاً. ووفقـاً للتقاريـر الأوليـة؛ يمكن استغلال هذه الثغرة عبر إرسـال بيانات معينة إلى واجهـة معينة فـي النظام، مما يـؤدي إلى تجاوز الحدود الأمنية للنظام، وتشغيل تعليمات برمجية غيـر مصرَّح بها مـن قبل. وهذا يعنـي أن المهاجم يمكـن أن يُثبّـت برمجيات خبيثـة، أو يُغيِّر إعدادات النظام، أو حتى يقوم بسـرقة بيانات حساسـة من الأجهزة المصابة.

تأثير هـذه الثغـرة لا يقتصـر على أجهـزة Linux الشـخصية فقط، بل يمتد ليشمل الخوادم الكبيرة التـي تُدير العديـد مـن المواقع والخدمـات عبر الإنترنت. ونظراً لاعتماد عدد كبير من الشركات على خوادم Linux لإدارة مواقعها وقواعد بياناتها؛ فإن استغلال هذه الثغرة قد يؤدي إلى تعطيل خدمات كبيرة أو سـرقة معلومات العملاء. وهذا يُشـكّل تهديداً كبيراً للبنية التحتية الحيوية التي تعتمد على Linux جزءاً من عملياتها اليومية.

شـركة Linux Foundation التـي تشـرف علـى تطوير النظام بالتعاون مـع مجتمع من المطورين العصريين سـارعت إلى إصـدار تحديث أمني بمجرد اكتشاف الثغرة. كما دعت جميع مستخدمي النظام إلـى تطبيق هذا التحديث في أسـرع وقتٍ ممكن للحمايـة من اسـتغلال الثغرة. في هذا السـياق، شـدَّدت الشـركة على أهمية التحديثـات الأمنية الدورية، وضرورة تطبيقهـا فور إصدارها، خاصةً مع تزايد تهديدات الهجمات السيبرانية المتطورة[1].

في ظل هذه الأحداث، يظهر مدى حساسية النُّظم التشـغيلية الكبـرى مثـل Linux أمـام الهجمات السـيبرانية. وعلى الرغم مـن أن نظام Linux يُعتبر عادةً من بين الأنظمة الأكثر أماناً؛ نظراً لآلية تطويره المفتوحة، واسـتجابة المجتمع السريعة للتحديات الأمنيـة؛ إلا أن الثغـرات لا تـزال تظهر بيـن الحين والآخر. هذه الحادثة تُشـدِّد على أهمية الاستمرار في البحث والتطوير لتعزيـز أمن الأنظمة مفتوحة المصدر مثل Linux.

يمكن القول: إن مثل هذه الثغرات المكتشـفة في Linux تُمثّـل تهديـداً حقيقياً يجـب التعامل معه بجديـة. ومع تزايـد الاعتماد على النظـم الرقمية المتصلة بالإنترنت، تصبح الهجمات التي تعتمد على اسـتغلال الثغرات البرمجية أكثر شـيوعاً وخطورةً. وعلى المستخدمين والشـركات على حدّ سواء أن يبقوا فـي حالة يقظـة دائمة، وأن يتخـذوا جميع التدابير الوقائية لضمان أمان أنظمتهم وبياناتهم.



1. Gatlan, Sergiu. CUPS flaws enable Linux remote code execution, but there's a catch, Bleeping Computer, , September 2024, on site: https://www.bleepingcomputer.com/news/security/cups-flaws-enable-linux-remote-code-execution-but-theres-a-catch/

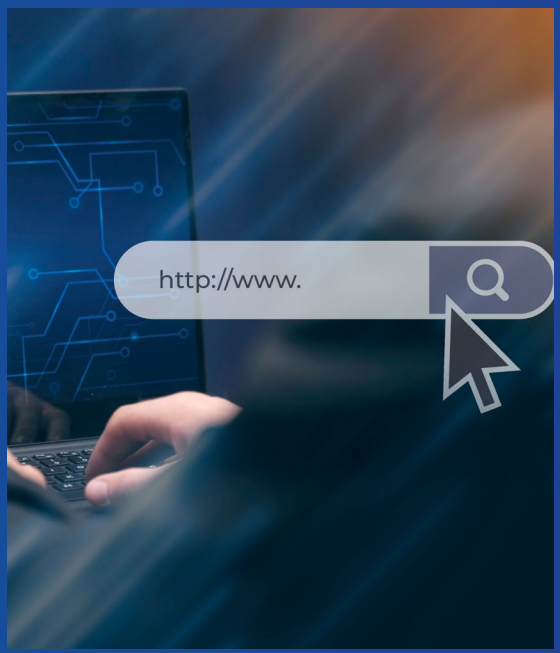
مؤتمر إدارة سطح الهجوم السيبراني

Attack Surface Management

في الآونة الأخيرة، أصبح مؤتمر إدارة سطح الهجوم السيبراني -الذي عُقِدَ افتراضياً بتاريخ 18 سبتمبر الماضي- حدثاً بارزاً يجمع بين المتخصصين في مجال الأمن السيبراني؛ لمناقشة التحديات المتزايدة التي تواجهها المؤسسات والشركات في عصر الهجمات الرقمية المتطورة. ويُعدّ هذا المؤتمر منصة رئيسة لتبادل الأفكار حول كيفية إدارة ما يُعرَف بـ"سطح الهجوم"، وهو مصطلح يشير إلى جميع النقاط أو الثغرات التي يمكن أن يستغلها المهاجمون لاختراق الأنظمة[1].

مؤتمر إدارة سطح الهجوم السيبراني Attack Surface Management يطرح استخدام أدوات متقدمة تعتمد على الذكاء الاصطناعي والتحليل الآلي

تأتي أهمية هذا المؤتمر في وقتٍ تتزايد فيه التهديدات السيبرانية بوتيرة سريعة؛ حيث تطورت أدوات الهجوم، وأصبحت أكثر تعقيداً وتنوعاً. مع تقدُّم التكنولوجيا، تتسع أيضاً فُرَص الهجمات، بدءاً من نقاط الضعف في البنية التحتية الرقمية إلى الأخطاء البشرية والإعدادات الأمنية غير المحمية. ويعمل المؤتمر على تقديم حلول مبتكَرة لمساعدة المؤسسات على تقييم وإدارة هذه المخاطر بشكل فعَّال.



واحدة من النقاط الرئيسة التي تم تناولها في هذا المؤتمر هي كيفية تحسين عملية تحديد وتقييم سطح الهجوم. ومن خلال استخدام أدوات متقدمة تعتمد على الذكاء الاصطناعي والتحليل الآلي؛ يمكن للشركات الحصول على صورة شاملة حول جميع الأجهزة والشبكات والتطبيقات المتصلة التي قد تكون عُرضة للاستغلال. ولذا فإن أحد الموضوعات التي نالت اهتماماً كبيراً مؤخراً هو كيفية الحدّ من سطح الهجوم عن طريق تقليل عدد الأجهزة غير الضرورية وتقوية الأنظمة الضعيفة.

1. https://www.securitysummits.com/event/attack-surface-management-summit/

إدارة سطح الهجوم أصبحت عنصراً أساسياً في إستراتيجيات الأمن السيبراني الحديثة؛ حيث أظهرت الأبحاث أن معظم الاختراقات السيبرانية تأتي من نقاط ضعف غير مرئية أو غير مدارة بشكل جيد. وتتبنَّى الشركات اليوم نهجاً متكاملاً لإدارة هذه النقاط الحساسة؛ حيث يتضمَّن ذلك مراقبةً مستمرةً وتحديثاً دورياً للتطبيقات والأنظمة. ما يُميّز هذا النهج هو القدرة على اتخاذ إجراءات استباقية بدلاً من ردّ الفعل التقليدي بعد وقوع الهجوم.

مؤتمر إدارة سطح الهجوم السيبراني.. منصة لتبادل الأفكار والحلول المبتكرة لمواجهة التحديات السيبرانية المتزايدة

تحدّث المتخصصون في المؤتمر عن أهمية التكامل بين تقنيات الحماية المختلفة، مثل جدران الحماية، وأدوات الكشف عن التسلل، وحلول إدارة الهوية والوصول، ضمن منصة مُوحَّدة لإدارة سطح الهجوم. هذا التكامل يُتيح للمؤسسات تحسين الرؤية الشاملة للأخطار المحتملة، ويقلل من مخاطر الهجمات الناجحة.

كما تناول المؤتمر مفهوم "الهجوم الداخلي"، أو ما يُعرَف بـ"الثغرات البشرية"؛ حيث يمكن أن تكون الأخطاء التي يرتكبها الموظفون أو الإجراءات غير الآمنة سبباً رئيساً للاختراقات. وتم التطرق إلى أهمية التوعية والتدريب المستمرَّيْن للموظفين حول كيفية التعامل مع الأنظمة بشكل آمِن وتجنُّب الوقوع في فخاخ التصيد الاحتيالي أو تنزيل البرمجيات الضارَّة.

وهناك جانب آخر تم تسليط الضوء عليه في المؤتمر؛ ألا وهو التحدي المتزايد الذي تفرضه التقنيات الحديثة مثل الحوسبة السحابية وإنترنت الأشياء (IoT). هذه التقنيات تفتح أفقاً جديداً للتطوير الرقمي، لكنها تزيد أيضاً من سطح الهجوم السيبراني. وتحدثت الشركات المشاركة عن كيفية تطوير إستراتيجيات لحماية البيانات المتنقلة والمنقولة بين الأنظمة المختلفة، بالإضافة إلى ضمان أمان الأجهزة المتصلة بالشبكات.

ختاماً، يُمثّل مؤتمر إدارة سـطح الهجوم السيبراني حدثـاً حيويـاً لتبـادل الأفـكار والحلـول المبتكَرة لمواجهة التحديات السيبرانية المتزايدة. ففي عالم متّصل بشكل متزايد، تحتاج الشركات إلى تبنّي نهج وقائي شـامل في إدارة سطح الهجوم السيبراني؛ لضمـان حماية أنظمتهـا وبياناتها الحساسـة من التهديدات الرقمية المتطورة.

الوكالة الوطنية للأمن السيبراني
National Cyber Security Agency

المبادرة الوطنيّة للسلامة الرقميّة
Digital Safety National Initiative

للتواصل مع إدارة التميُّز السيبراني الوطني


00974 404 663 79


00974 404 663 62


www.ncsa.gov.qa/


cyberexcellence@ncsa.gov.qa