شركة MITSUBISHI ELECTRIC
قسم العلاقات العامة
7-3, Marunouchi 2-chome, Chiyoda-ku, Tokyo, 100-8310 Japan

بالنسبة للنشرة الفورية **رقم ٣٦٤٩**

إن هذا النص ترجمة للنص الإنجليزي الرسمي لهذا الإصدار الجديد، وقد تم تزويده للرجوع إليه بسهولة عند الحاجة. يرجى الرجوع إلى النص الإنجليزي الأصلي للحصول على التفاصيل و/أو المواصفات الخاصة. في حال وجود أي تعارض، فيجب اتباع محتوى الإصدار الإنجليزي الأصلي.

استفسارات العملاء

مركز البحث والتطوير لتقنية المعلومات
شركة Mitsubishi Electric

www.MitsubishiElectric.com/ssl/contact/company/rd/form.html

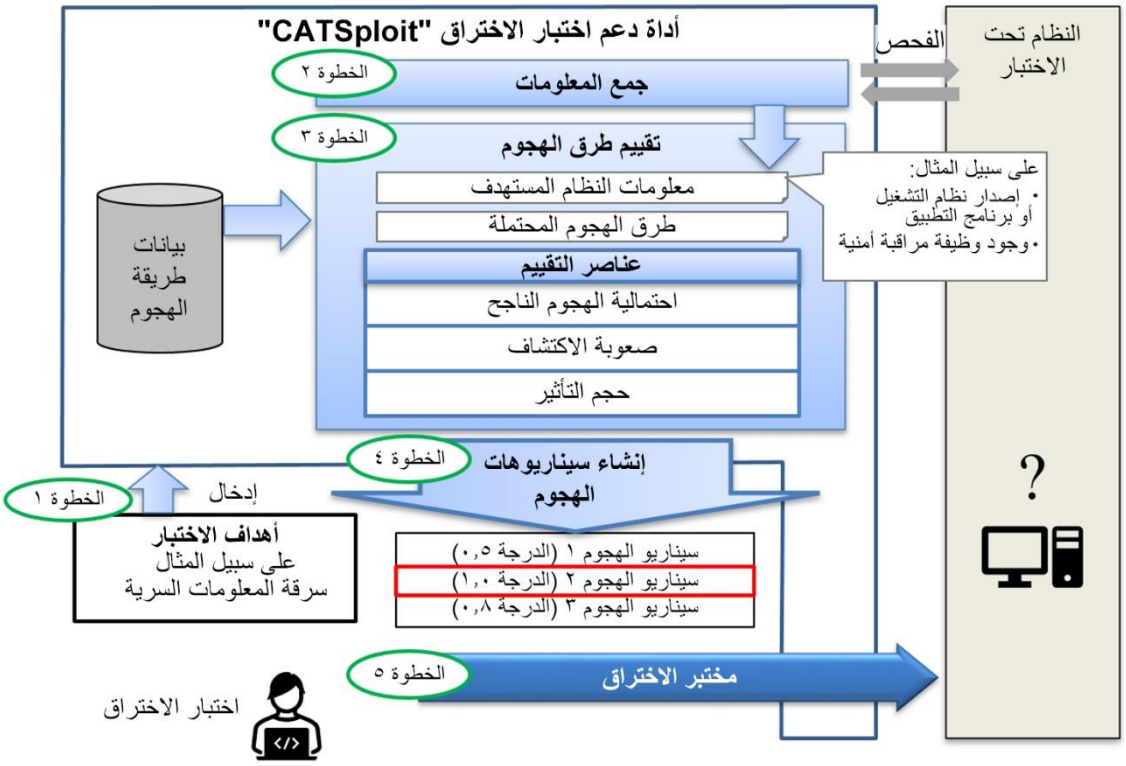
الاستفسارات الإعلامية

قسم العلاقات العامة
شركة Mitsubishi Electric

prd.gnews@nk.MitsubishiElectric.co.jp
www.MitsubishiElectric.com/news/

شركة Mitsubishi Electric تنشئ أول أداة لدعم اختبار الاختراق في العالم، والتي تعمل على إنتاج سيناريوهات الهجوم من منظور المخترقين

من المتوقع أن تؤدي إلى تحسين قدرة جميع المنتجات المتصلة بالشبكات على التصدي للهجمات الإلكترونية



مثال لاستخدام أداة الدعم أثناء اختبار الاختراق

طوكيو، ٥ ديسمبر ٢٠٢٣ – أعلنت شركة Mitsubishi Electric (طوكيو: ٦٥٠٣) اليوم إنشائها لأول أداة في العالم[١] لدعم اختبار الاختراق[٢] يُطلق عليها CATSploit، وهي تقوم تلقائيًا بإنتاج سيناريوهات الهجوم استنادًا إلى أهداف الاختبار التي وضعها مختبر الاختراق، مثل سرقة المعلومات السرية، لتقييم مدى تأثير الهجمات موضع الاختبار. ومن خلال الاستعانة بسيناريوهات الهجوم ونتائج الاختبار الناتجة (الدرجات)، يمكن حتى لمهندسي الأمن الذين لا يتمتعون بالخبرة إجراء اختبارات الاختراق بسهولة.

[١] وفقًا للبحث الذي أجرته شركة Mitsubishi Electric في ٥ ديسمبر ٢٠٢٣
[٢] اختبار للتأكد من إمكانية اختراق النظام أو المعدات من خلال هجوم فعلي

في السنوات الأخيرة، أصبحت أنظمة التحكم، بما في ذلك البنية التحتية ومعدات المصانع وما إلى ذلك، تعتمد بشكل متزايد على الاتصال بالشبكات، مما يزيد من مخاطر حدوث أعطال، مثل انقطاع التيار الكهربائي أو تعطل وسائل النقل العام، بسبب الهجمات السيبرانية. وقد أصبح تنفيذ تدابير أمنية في مثل هذه الأنظمة أمرًا مُلحًا. بالإضافة إلى ذلك، تتطلب معايير ISA/IEC 62443[٣] إجراء اختبارات الفحص العشوائي[٤] والاختراق الأمنية على الأنظمة والمعدات لتقييم قدرتها على التصدي للهجمات الإلكترونية، وتشمل تحديد الثغرات الأمنية الناتجة عن أخطاء وقعت في مرحلة التنفيذ أو التكوين. يُعد اختبار الاختراق اختبارًا معقدًا للغاية ويتطلب مشاركة قراصنة القبعات البيضاء[٥] لمهاجمة النظام أو المنتج الذي يتم اختباره بشكل فعلي، ولكن هؤلاء الأفراد، الذين يجب أن يمتلكوا مستويات عالية للغاية من الخبرة، نادرون ويصعب العثور عليهم.

قامت شركة Mitsubishi Electric، من خلال التركيز على العوامل التي يأخذها قراصنة القبعات البيضاء في الاعتبار عند اختيار متجهات الهجوم الخاصة بهم، بتطوير أداة دعم لاختبار الاختراق تقوم بإنشاء قوائم بسيناريوهات الهجوم المحتملة ومدى تأثيرها (يتم التعبير عنها كدرجات عددية).

سيتم عرض تفاصيل الأداة في ٦ ديسمبر (١١ صباحًا بالتوقيت المحلي) خلال مؤتمر Black Hat Europe Arsenal لعام ٢٠٢٣ في لندن، والذي سيقام يومي ٦ و٧ ديسمبر.

<u>الميزات</u>

1) تقوم تلقائيًا بإنشاء سيناريوهات الهجوم من منظور قراصنة القبعات البيضاء

- ركزت شركة Mitsubishi Electric على العوامل التي يأخذها قراصنة القبعات البيضاء في الاعتبار عند اختيار أساليب الهجوم الخاصة بهم، مثل احتمالية الهجوم الناجح، وصعوبة الاكتشاف، وحجم التأثير. من خلال التعديل في ضوء الأهداف الموضوعة لإجراء اختبارات محددة، يستطيع النظام إنشاء سيناريوهات تلقائيًا توضح الخطوات اللازمة لتنفيذ هجوم من شأنه تحقيق تلك الأهداف.

2) تقوم الاختبارات المثالية بتقييم مدى فعالية سيناريوهات الهجوم من منظور قراصنة القبعات البيضاء

- تقوم طريقة CATS[٦] المسجلة ملكيتها لشركة Mitsubishi Electric بحساب فعالية كل طريقة هجوم (يتم التعبير عنها كدرجات عددية) من منظور أحد قراصنة القبعات البيضاء، بناءً على قائمة من سيناريوهات الهجوم المقترحة بحيث يمكن اختيار السيناريو الأكثر فعالية (أعلى درجة).
- لا يأخذ تقييم CATS في الاعتبار معلومات النظام المعروفة فحسب، مثل نظام التشغيل وإصدار التطبيق وأجهزة مراقبة الأمان، بل يأخذ أيضًا معلومات النظام المفقودة، مما يساعد على تنفيذ سيناريوهات الهجوم التي تحاكي بشكل وثيق منظور المهاجم الفعلي.
- ويمكّن التقييم الآلي لسيناريوهات الهجوم التي من المحتمل أن يستخدمها قراصنة القبعات البيضاء مهندسي الأمن الأقل خبرة من إجراء اختبارات الاختراق بسهولة.

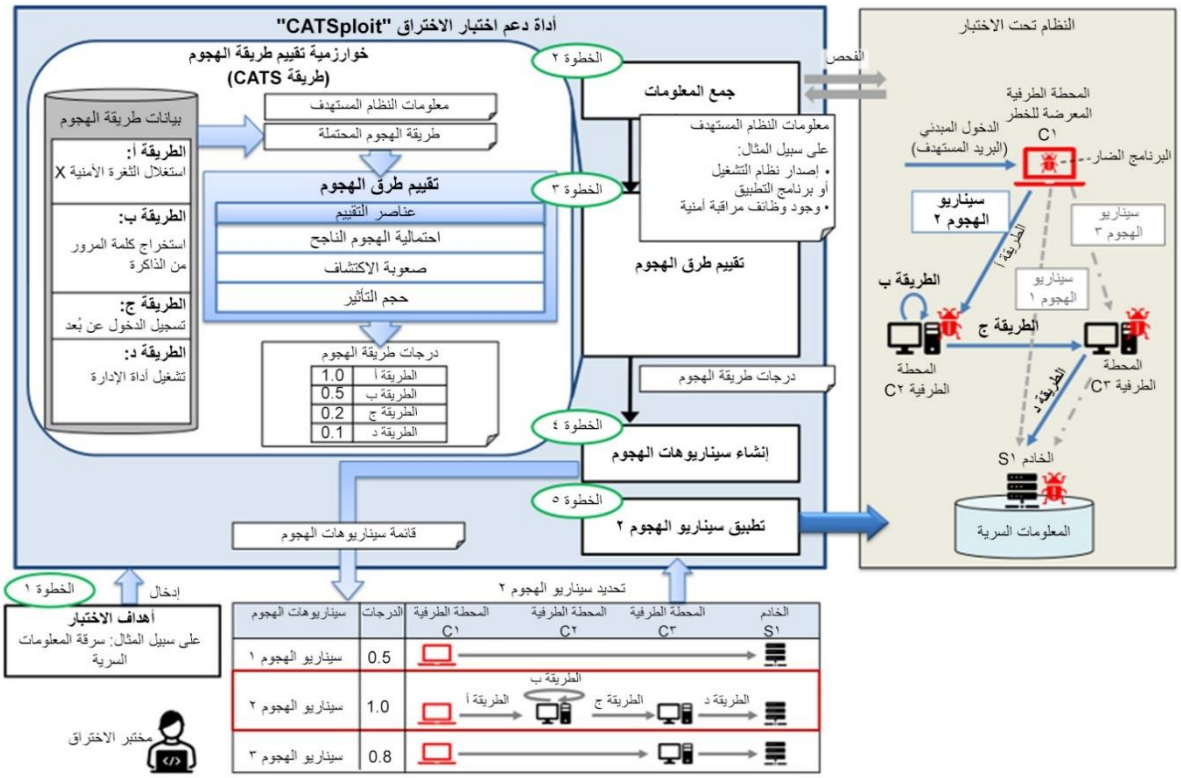
---

[٣] المعايير الأمنية لأنظمة التحكم الصناعية

[٤] طريقة اختبار لاكتشاف عيوب البرامج أو نقاط الضعف عن طريق إدخال بيانات غير صالحة أو غير صحيحة

[٥] قراصنة الأمن الأخلاقي الذين يستخدمون المعرفة المتقدمة وتكنولوجيا الكمبيوتر لتحديد المشكلات الأمنية وما إلى ذلك.

[٦] درجات تقنيات الهجوم السيبراني: طريقة مملوكة لشركة Mitsubishi Electric لتقييم فعالية متجهات الهجوم



أداة دعم اختبار الاختراق CATSploit

التطوير المستقبلي

لزيادة تحسين قدرة الأنظمة والأجهزة التي طورتها شركة Mitsubishi Electric على التصدي للهجمات الإلكترونية، ستواصل الشركة إجراء اختبارات على هذه الأداة الجديدة وتطويرها بهدف استخدامها في اختبار الأمان الفعلي لمنتجات الشركة بحلول عام ٢٠٢٦.

###

نبذة عن شركة Mitsubishi Electric

مع أكثر من ١٠٠ عامًا من الخبرة في مجال توفير منتجات موثوق بها وعالية الجودة، تعد شركة Mitsubishi Electric (طوكيو: ٦٥٠٣) شركة رائدة عالميًا معترف بها في مجال تصنيع وتسويق وبيع المعدات الكهربائية والإلكترونية المستخدمة في معالجة المعلومات والاتصالات وتنمية الفضاء والاتصالات عبر الأقمار الصناعية والإلكترونيات الاستهلاكية والتكنولوجيا الصناعية والطاقة والنقل ومعدات البناء. تُثري شركة Mitsubishi Electric المجتمع بالتكنولوجيا انطلاقًا من بيانها "التغيير نحو الأفضل". وقد سجلت الشركة حجم مبيعات بمقدار ٥٠٠٣,٦ مليار ين (٣٧,٣ مليار دولار أمريكي*) في السنة المالية المنتهية في ٣١ مارس ٢٠٢٣. وللمزيد من المعلومات، تفضل بزيارة الموقع www.MitsubishiElectric.com

*يتم تحويل المبالغ بالدولار الأمريكي من الين بسعر صرف ¥١٣٤ ينًا =١ دولار أمريكي، وهو السعر التقريبي المُعطى من قبل سوق طوكيو لتبادل العملات الأجنبية في ٣١ مارس ٢٠٢٣