مصرف الإمارات العربية المتحدة المركزي
CENTRAL BANK OF THE U.A.E.

سياسة الإفصاح عن نقاط الضعف

سياسة الإفصاح عن نقاط الضعف

المعلومات الخاصة بالمستند	
عنوان السياسة:	سياسة الإفصاح عن نقاط الضعف

تاريخ التعديلات				
رقم التعديل	تاريخ الإصدار	ملخص التغييرات	الأقسام	تم إجراء التغييرات من قبل:
0.1	29 يوليو 2021	النسخة الأولية	لا ينطبق	فريق أمن المعلومات
0.2	7 فبراير 2022	النسخة النهائية	لا ينطبق	فريق أمن المعلومات

جدول المحتويات

مقدمة

يتبنى مصرف الإمارات العربية المتحدة المركزي ثقافة قائمة على الأداء حيث يوجه جميع موظفيه إلى أهمية وضع خلل سعيه للحفاظ على أمن أنظمته المالية، يتولى مصرف الإمارات العربية المتحدة المركزي ("المصرف المركزي") المسؤولية عن حماية البيانات. تشتمل هذه السياسة الخاصة بالإفصاح عن نقاط الضعف على مبادئ توجيهية ذات شفافية مخصصة للباحثين، لتمكينهم من اكتشاف نقاط الضعف في الحماية الأمنية، وتُوفّرُ نبذةً عامةً واضحة عن كيفية إبلاغنا بأي نقاط ضعف تمّ تحديدها.

تشتمل هذه السياسة أيضاً على وصفٍ لأنواع ونظم البحوث المشمولة، وعلى إجراءٍ لتزويدنا بتقاريرٍ حول نقاط الضعف، وعلى الشروط الخاصة بإجراءات نقاط الضعف، بما في ذلك فترة انتظار الباحثين الأمنيين قبل الإفصاح للجمهور عن نقاط الضعف التي تم الإبلاغ عنها.

نُرحّبُ ونشجعكُم على إرسال تقارير لنا لضمان الإفصاح عن أي نقاط ضعف محتملة في النظام ومعالجتها.

1 التصريح

بشرط التقيد بأحكام هذه السياسة خلال قيامك بالبحث الأمني، فإننا سنضمن تعاوننا معك للحصول على فهم شامل لإدراك حقيقة المشاكل وحلها في أسرع وقتٍ ممكن. وفي مثل هذه الحالات، سيتم اعتبار بحثك بأنه مُصرّحٌ له، ولن يسعى المصرف المركزي أو يوصي باتخاذ إجراء قانوني يتعلق بالبحث الذي تم إجراؤه. إذا قام طرفٌ ثالث برفع دعوى قضائية ضدك تتعلق بأنشطة أبحاث الأمن المتوافقة مع سياستنا، فإننا سنعلنُ بأنه تم التصريح لك.

2 الإرشادات

في إطار عمل هذه السياسة، فإن مصطلح «البحث» يشمل الأنشطة التي تستوفي الشروط التالية:

- لقد قمت بتزويدنا بإشعار فوري حول اكتشاف أي مشكلة أمنية أو مشكلة محتملة؛
- لقد بذلت ما بوسعك لمنع انتهاك خصوصيتك، والتلاعب بالبيانات، وتدمير المعلومات، وتراجع تجربة المستخدم، وزعزعة استقرار نظام الإنتاج؛
- لقد عملت فقط في إطار السياق المطلوب لتأكيد مسألة الضعف الكائنة. ولا يجب استخدام أي ميزات لاستعراض البيانات أو تقديم تنازلات بشأنها أو الانتقال لنظام مختلف أو تحديد إمكانية وصول مستمرة إلى سطر الأوامر؛
- قمت بالسماح لنا بتوفير حلٍ في غضون فترة زمنية معقولة، قبل الإفصاح للجمهور عن مسألة الضعف؛
- قمت بتقديم تقرير ملائمٍ من حيث حجم التقرير وجودته. يرجى منحنا وقتاً كافياً لحل المشكلة قبل الإفصاح عنها للجمهور؛
- لم تقم بإرسال عددٍ كبيرٍ من التقارير ذات الجودة المنخفضة.

عند تحديد نقطة ضعف موجودة، أو عند وجود بيانات حساسة مثل التفاصيل المالية، والتفاصيل الشخصية، والأسرار التجارية، أو البيانات المملوكة بشكل خاص من قبل أي طرف، فإننا نتوقع منك إبلاغنا بذلك فوراً، دون أي إفصاح إضافي عن نقطة الضعف التي تم تحديدها أو مواصلة اختبار وجود نقطة الضعف.

3 أساليب الاختبار

إننا لا نوفرُ تصريحاً لإجراء اختبارٍ بالطرق التالية:

- الاختبارات غير الفنية، وتحديداً الهندسة الاجتماعية (مثل التجسس والتصيد الاحتيالي، وما إلى ذلك)، والاختبارات الفعلية (مثل الوصول غير المصرح له والأبواب المفتوحة وإمكانية الوصول إلى المكاتب، وغير ذلك)؛
- اختبار نقطة ضعف في مواقع إلكترونية أو خدمات أو تطبيقات تابعة لطرفٍ ثالثٍ وذات علاقة بأنظمة المصرف المركزي أو في تلك الأنظمة أو مدمجة فيها؛
- اختبارات هجمات قطع الخدمة أو اختبارات الهجمات المشتركة لقطع الخدمة أو أي اختبارات أخرى لهجمات قطع الخدمة على الشبكة تؤدي لإحداث ضرر في البيانات أو الأنظمة ذات الصلة، وتمنْع الوصول إليها؛
- أنظمة اختبار تختلف عن تلك المذكورة في قسم "نطاق العمل" أدناه؛
- الاختبار الذي قد يتسبب في انقطاعٍ متعمدٍ أو توقف عمل أو إعاقة لنظم المصرف المركزي أو يؤدي إلى تراجع عمل النظام في المصرف المركزي؛
- الاختبار الذي يسمح باستخدام برامج ضارة؛
- الاحتفاظ ببيانات المصرف المركزي أو مشاركتها أو تعديلها أو حذفها؛
- رفض الوصول إلى بيانات المصرف المركزي؛ أو
- الاختبار باستخدام أدواتٍ تهدُف إلى استعراض البيانات أو الانتقال لنظام مختلف في المصرف المركزي أو تحديد إمكانية وصول مستمرة إلى سطر الأوامر أو مواصلة الاستخدام الدائم لأنظمة المصرف المركزي.

4 نطاق العمل

يقتصرُ تطبيق هذه السياسة على الخدمات والأنظمة التالية:

- *.cbuae.gov.ae, *.centralbank.ae,

لا يتوفر التصريح المطلوب لإجراء اختبار إلا بخصوص الخدمات الواردة في القائمة أعلاه، حيث تم إدراجها في نطاق العمل المسموح به. وهذا لا يشمل أي نقاط ضعفٍ محددة في أنظمة الموردين الذين نتعامل معهم؛ وفي هذه الحالات، يتم إرسال تقرير مماثل إلى المورد المعني مع التقيد الصارم بسياسة الإفصاح عن نقاط الضعف، إن وجدت.

إننا نطلُب إجراء اختبارات وإعداد بحوث ذات فعالية فقط في نطاق الخدمات والنظم المشمولة بهذه السياسة، بغض النظر عما إذا كنا مشاركين في تطوير وصيانة خدماتٍ ونظمٍ أخرى تستند إلى الإنترنت. كما أننا نشجّعكم على اطلاعنا على حالات القلق التي تساوركم لإجراء مزيد من النقاش حول أي نظمٍ خارج نطاق العمل المذكور أعلاه، ونعتقد أنها تتطلب إجراء اختبار.

5 الإبلاغ عن نقطة ضعف

يتمثّلُ الغرض الوحيد من التقارير المقدمة طبقاً لهذه السياسة للإفصاح عن نقاط الضعف في ضمان حماية البيانات، وكذلك تصحيح جميع نقاط الضعف الكائنة أو التخفيف من حدتها. إذا كانت نتائج بحثك تغطي أي نقاط ضعفٍ لم تكن معروفةً من قبل وتؤثر على المصرف المركزي أو على خدماته أو على مستخدمي منتجاته، فإننا سندرس إمكانية مشاركتها مع وكالات الأمن السيبراني الحكومية، أو المنظمات التجارية، أو فريق الاستجابة لطوارئ الحاسب الآلي أو مع كيانات أخرى للبدء بعملية رسمية للإفصاح عن نقاط الضعف، وفقا لسياساتهم. إننا سنقوم بالكشف عن تفاصيل الاتصال الخاصة بك أو اسمك فقط إذا كنت قد أعطيتنا الموافقة المطلوبة على ذلك.

يمكنك إرسال تقاريرك بشكل مجهول، حيث نقبل التقارير إما عن طريق البريد الإلكتروني information.security@cbuae.gov.ae أو من خلال نموذج تقرير الإبلاغ عن نقاط الضعف على موقع الإنترنت.

سوف تستلم تأكيداً باستلام التقرير في غضون ثلاثة أيام عملٍ من مشاركة تفاصيل الاتصال الخاصة بك معنا.

1.5 ما الذي نتوقعه منك

إن المعالجة السليمة وترتيب أولويات التقارير المقدّمة تتطلب منك التقيّد بالشروط التالية:

- وصف تفصيلي لموقع نقطة الضعف، والأثر المحتمل لاستخدامها؛
- يُرجى إرسال لقطات للشاشة وإثباتات لسيناريو مفهوم نقطة الضعف مع عرضٍ تفصيلي للتدابير اللازمة لمعالجة نقطة الضعف؛
- إننا نُفضّلُ إعداد التقارير باللغة الإنجليزية، إذا كان ذلك ممكناً.

2.5 ما الذي يمكنك توقعه منا

إذا قُمت بمشاركة معلومات الاتصال الخاصة بك معنا، فإننا نضمنُ تواصلاً ذو شفافيةٍ دون أي تأخير:

- نقوم بإرسال إقرارات باستلام التقارير في غضون ثلاثة أيام عمل؛
- نُوفّرُ التأكيد المطلوب بشأن نقطة الضعف، بأفضل طريقةٍ ممكنة، كما أننا نضمنُ أكبر قدرٍ من الشفافية للتدابير المتخذة في سياق أي عملية معالجة لنقطة الضعف، إلى جانب تغطية التحديات والمسائل المحتملة المرتبطة بحل مسألة نقطة الضعف.
- إننا نضمنُ تواصلاً يتسم بانفتاحية لمناقشة جميع مسائل نقطة الضعف.

6 الأسئلة

سوف نقوم بالإجابة على الأسئلة المرسلة على البريد الإلكتروني information.security@cbuae.gov.ae حول هذه السياسة، كما أننا سنأخذُ ملاحظاتك واقتراحاتك بعين الاعتبار عند إرسال الردود المحتملة.