Guatemala - El Salvador - Honduras - República Dominicana

Devel
CYBERSECURITY REDEFINED

CYBER SECURITY NEWS

SECURITY OPERATIONS CENTER

EL CHATBOT DE CONTRATACIÓN DE MCDONALD'S EXPONE DATOS DE MILLONES DE SOLICITANTES

10/ 07 / 2025

CONTENIDO

Introducción

Esta noticia expone un fallo crítico en la seguridad básica: una base de datos con información sensible, protegida por una contraseña tan trivial como "123456", fue encontrada **expuesta al público**.

Este incidente no solo subraya los peligros de una configuración de seguridad deficiente, sino que también nos invita a reflexionar sobre la responsabilidad de las empresas al manejar datos personales y la importancia vital de la ciberseguridad en un mundo cada vez más interconectado. La historia de la IA de contratación de McDonald's es un recordatorio contundente de que, en la carrera por la eficiencia tecnológica, la seguridad nunca debe ser un pensamiento secundario.

EL CHATBOT DE CONTRATACIÓN DE MCDONALD'S EXPONE DATOS DE MILLONES DE SOLICITANTES

A continuación, se encuentra en cuadro de identificación de la amenaza.

ID de alerta:	DSOC-CERT_2025_07_10_1
Clasificación de alerta:	Noticia
Tipo de Impacto:	Alta
TLP (Clasificación de información):	**CLEAR**
Fecha de publicación:	10/07/2025
Es día cero (0 day):	No

RESUMEN

McDonald’s siendo una empresa grande a nivel mundial optó por tratar de automatizar varias de las operaciones que poseen, una de las inversiones que hicieron fue apostar por un chatbot para agilizar así el proceso de contratación de personal.

Para poder cumplir con esto de manera eficiente McDonald’s contrató a una empresa estadounidense especializada en soluciones de IA para recursos humanos, el producto en cuestión es un asistente virtual de contratación, se encarga de recopilar información, responder preguntas, programar entrevistas entre otras tareas.

¿Qué sucedió?

Investigadores encontraron que los datos recolectados por el chatbot estaban almacenados en una base de datos de Mongo DB expuestas y sin protección adecuada.

Lo más alarmante de todo el incidente es que la contraseña para ingresar a los datos era increíblemente sencilla, la contraseña utilizada era: 123456. Esto es sumamente crítico ya que cualquier persona con un conocimiento bastante básico sobre bases de datos e IP pudo haber accedido a la información.

La base de datos contenía información de millones de solicitantes de empleo según lo que se sabe la cifra seria 64 millones de registros, aunque el número podría llegar a variar.

¿Qué tipos de datos fueron expuestos?

- Nombres completos
- Direcciones de correo electrónico
- Números de teléfono
- Historial de solicitudes de empleo
- Respuestas a preguntas de selección (aunque no se especifica si eran preguntas muy personales, cualquier información relacionada con el empleo es sensible).

¿Cuál es la raíz del problema?

La falta de una contraseña robusta para proteger la base de datos es uno de los errores más importantes de todo el incidente, a pesar de que se utiliza una base de datos crítica pudieron haber eludido parte del problema con una contraseña compleja y única, como autenticación multifactorial u otros tipos de mecanismos de seguridad.

Dejando de lado la contraseña débil, la base de datos no debería haber sido accesible desde internet sin **restricciones de IP o firewalls adecuados. Esto sugiere una mala gestión por parte del grupo de infraestructura.**

RECOMENDACIONES

- Configuraciones seguras por defecto: Asegúrate de que todos los sistemas, bases de datos y servicios en la nube vengan con las configuraciones de seguridad más estrictas habilitadas por defecto, en lugar de depender de configuraciones manuales posteriores.

- Contraseñas complejas y únicas: Exige y haz cumplir el uso de contraseñas largas, complejas y únicas para todas las cuentas, especialmente aquellas con acceso a datos sensibles o a la administración de sistemas.

- Autenticación Multifactorial (MFA): Implementa MFA para todos los accesos administrativos y para cualquier cuenta que maneje datos críticos. Esto añade una capa de seguridad crucial, requiriendo una segunda verificación (ej. código del móvil) además de la contraseña.

- No expongas bases de datos a internet: Por defecto, las bases de datos no deberían ser accesibles directamente desde la web pública. Utiliza firewalls, VPNs y listas de control de acceso (ACLs) para restringir el acceso solo a direcciones IP autorizadas.

NOTICIA COMPLETA

https://devel.group/blog/el-chatbot-de-contratacion-de-mcdonalds-expone-datos-de-millones-de-solicitantes/

CONTACTOS DE SOPORTE

Correo electrónico: cti@develsecurity.com

Teléfonos directos:

Guatemala: +(502) 2307 5757

El Salvador: +(503) 2249 4252

Honduras: +(504) 2283 5904

República Dominicana: +1 829 734 2040

WhatsApp: +(502) 5124 9536

Sitio Web: https://devel.group