Guatemala - El Salvador - Honduras - República Dominicana

Devel
CYBERSECURITY REDEFINED

CYBER SECURITY NEWS

SECURITY OPERATIONS CENTER

UN NUEVO INCIDENTE DE CIBERSEGURIDAD AFECTA A EQUIFAX

16 / 07 / 2024

CONTENIDO

INTRODUCCIÓN

En un reciente incidente de ciberseguridad, Equifax ha sido nuevamente objeto de una posible filtración de datos, según lo revelado por IntelBroker en BreachForums, una conocida comunidad de actividades criminales en línea. El actor de amenazas afirma haber exfiltrado aproximadamente 100 líneas de datos de un bucket de almacenamiento Azure de la empresa, lo que incluye información personal y laboral de los usuarios. A pesar del alcance limitado de la violación, este evento subraya la necesidad continua de medidas de seguridad robustas para proteger datos sensibles, especialmente en organizaciones que manejan información financiera crítica.

UN NUEVO INCIDENTE DE CIBERSEGURIDAD AFECTA A EQUIFAX

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

ID de alerta:	DSOC-CERT_2024_07_16_1
Clasificación de alerta:	Noticia
Tipo de Impacto:	Alta
TLP (Clasificación de información):	**CLEAR**
Fecha de publicación:	16/07/2024
Es día cero (0 day):	No

RESUMEN

Recientemente, un actor de amenazas en un foro clandestino ha publicado un supuesto filtrado de datos. Este incidente fue revelado por IntelBroker en BreachForums, una comunidad en línea conocida por actividades criminales cibernéticas. Según IntelBroker, los datos fueron obtenidos de un bucket de almacenamiento Azure de staging de Equifax.

DETALLES DEL PRESUNTO INCIDENTE

De acuerdo con la publicación de IntelBroker, la violación implicó la exfiltración de algunos archivos de un bucket de almacenamiento Azure de Equifax. El actor de amenazas afirma haber perdido el acceso durante la exfiltración de los datos y solo logró extraer aproximadamente 100 líneas de datos de usuarios. Estos datos incluyen supuestamente las siguientes cabeceras: ID, nombre, apellido, correo electrónico, puesto y departamento. La publicación incluye una lista parcialmente oscurecida de estas entradas, subrayando el alcance limitado de la violación.

CONTEXTO DE EQUIFAX Y EL IMPACTO POTENCIAL

Equifax, una empresa global de análisis de datos y tecnología, es una de las agencias de crédito más grandes del mundo. Con operaciones en numerosos países y una fuerza laboral de miles de personas, Equifax gestiona enormes cantidades de datos financieros sensibles. La empresa desempeña un papel crucial al proporcionar puntuaciones e informes de crédito, fundamentales para diversas transacciones y decisiones financieras.

Los actores de amenazas que apuntan a organizaciones como Equifax a menudo buscan robar información personal y financiera valiosa. Estos datos pueden ser vendidos en mercados clandestinos o utilizados para robos de identidad, fraudes financieros y otras actividades maliciosas. La violación de un bucket de almacenamiento de Equifax, aunque de pequeña escala como se afirma, resalta los continuos esfuerzos de los criminales cibernéticos por explotar las vulnerabilidades en grandes corporaciones.

IMPLICACIONES DE LA VIOLACIÓN

La divulgación de información personal, incluso en cantidad limitada, conlleva riesgos significativos. Los datos compartidos por IntelBroker incluyen información identificable como nombres, correos electrónicos y puestos de trabajo. Esta información puede ser utilizada para realizar ataques de phishing, robos de identidad y otras formas de criminalidad cibernética. Además, la exposición de las afiliaciones departamentales podría proporcionar un contexto adicional para ataques de ingeniería social dirigidos a empleados o asociados de Equifax.

Este incidente subraya la importancia de contar con medidas de seguridad robustas y una vigilancia constante en la protección de datos sensibles. Organizaciones como Equifax, que manejan información financiera crítica, deben garantizar que sus sistemas de almacenamiento estén adecuadamente protegidos contra accesos no autorizados.

ANTECEDENTES DE EQUIFAX: EL MASIVO LEAK DE DATOS DE 2017

En 2017, Equifax estuvo en el centro de uno de los ataques cibernéticos más grandes y devastadores de la historia. El incidente, que afectó a aproximadamente 147 millones de personas, fue causado por una

vulnerabilidad en el framework Apache Struts2, utilizado por la empresa para algunas de sus aplicaciones web. Esta vulnerabilidad, conocida como CVE-2017-5638, permitía la ejecución de código remoto, lo que permitió a los atacantes enviar comandos maliciosos al servidor web de Equifax y obtener acceso no autorizado a datos sensibles.

El ataque tuvo consecuencias significativas no solo para las personas afectadas, sino también para la propia Equifax. La empresa enfrentó numerosas demandas legales, una pérdida de confianza por parte de los consumidores y una revisión exhaustiva de sus prácticas de seguridad. El incidente destacó la crucial importancia de la gestión rigurosa de vulnerabilidades y la actualización oportuna de sistemas, especialmente cuando se trata de proteger datos críticos y sensibles.

CONCLUSIÓN

Aunque la presunta violación de datos de Equifax reportada por IntelBroker en BreachForums sigue sin confirmarse, sirve como un recordatorio contundente de las amenazas persistentes que enfrentan las organizaciones que gestionan información sensible.

En RHC Dark Lab, continuaremos monitoreando la evolución de la situación para publicar más noticias en el blog si hay actualizaciones sustanciales. Si hay individuos con conocimiento de los hechos que deseen proporcionar información de manera anónima, pueden utilizar nuestro correo electrónico cifrado para informantes.

Este artículo se ha compilado con base en información pública que aún no ha sido verificada por las organizaciones respectivas. Actualizaremos a nuestros lectores a medida que estén disponibles más detalles.

NOTICIA COMPLETA

https://devel.group/blog/un-nuevo-incidente-de-ciberseguridad-afecta-a-equifax/

CONTACTOS DE SOPORTE

Correo electrónico: cert@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://www.devel.group/reporta-un-incidente