Natura, la compañía de cosméticos más grande de Brasil, accidentalmente expuso cientos de GB de información personal y relacionada con pagos de sus clientes, a la que se pudo acceder de forma pública en línea por cualquier persona sin necesidad de autenticación.

El investigador de SafetyDetective, Anurag Sen, descubrió el mes pasado dos servidores alojados en Amazon sin protección, con 272 GB y 1.3 TB, pertenecientes a Natura, que constaban de más de 192 millones de registros.

Según el informe de Anurag, los datos expuestos incluyen información de identificación personal de 250 mil clientes de Natura, las cookies de inicio de sesión de sus cuentas, además de los archivos que contienen registros de los servidores de usuarios.

Es preocupante que la información filtrada también incluye los detalles de cuenta de pago Moip con tokens de acceso para casi 40 mil usuarios de wirecard.com.br integradas con cuentas Natura.

> *«Alrededor del 90% de los usuarios eran clientes brasileños, aunque también estaban presentes otras nacionalidades, incluidos clientes de Perú»,* dijo Anurag.
>
> *«El servidor comprometido contenía registros de API del sitio web y del sitio móvil, exponiendo así toda la información del servidor de producción. Además, se mencionaron varios nombres de cubo de Amazon en la filtración, incluidos documentos PDF que se refieren a acuerdos formales entre varias partes»,* agregó.

Entre la información expuesta se encontró:

- Nombres completos
- Nombres de solteras
- Fechas de nacimiento
- Nacionalidad

- Género
- Contraseñas hash de inicio de sesión
- Detalles de la cuenta MOIP
- Credenciales de API con contraseñas sin cifrar
- Compras recientes
- Números de teléfono
- Correos electrónicos y direcciones físicas
- Tokens de acceso para wirecard

Además, el servidor desprotegido también tenía un archivo secreto de certificado .pem que contiene la contraseña para el servidor EC2 Amazon donde está alojado el sitio web de Natura.

De ser explotado, la clave del servidor podría haber permitido a los hackers inyectar directamente un skimmer digital en el sitio web oficial de la compañía para robar los datos de tarjetas bancarias de los usuarios en tiempo real.

> *«Los detalles expuestos sobre el backend, así como las claves de los servidores, podrían aprovecharse para realizar más ataques y permitir una penetración más profunda en los sistemas existentes»*, dijo el investigador.

SafetyDetective intentó informar sobre los hallazgos de su investigador directamente a la compañía afectada el mes pasado, pero no recibió ninguna respuesta a tiempo, luego de esto, se contactó con los servicios de Amazon, donde pidió a la compañía que asegurara los servidores inmediatamente.

Hasta ahora no se sabe si un servidor malicioso también accedió a los servidores desprotegidos y a los datos confidenciales almacenados antes de desconectarse.

> *«Las instancias de información de identificación personal expuestas podrían*

> *conducir al robo de identidad y al fraude, ya que pueden ser utilizadas por los atacantes para su identificación en distintos sitios y ubicaciones. La fuga de datos de Natura también aumenta el riesgo de phishing y estafas telefónicas»,* dijo el investigador.