



Baptch Robert Robert, investigador de seguridad que trabaja bajo el seudónimo «Elliot Alderson», con ayuda de un investigador indio que prefiere permanecer anónimo, descubrió que el sitio web oficial de la popular compañía estatal de gas LPG Indane, filtra información personal de sus millones de clientes, incluyendo sus número de Aadhaar.

Esta no es la primera vez que una base de datos de terceros sin protección filtra detalles de Aadhaar de los ciudadanos indios, que es un número único asignado a cada ciudadano como parte del programa de identidad biométrica de la India mantenido por la Autoridad de Identificación Única de India (UIDAI).

A inicios de esta semana, un investigador anónimo de la India descubrió inicialmente una laguna en el portal de distribuidores en línea de Indane que podía permitir a cualquier persona acceder a cientos de miles de datos de clientes asociados con sus respectivos distribuidores sin necesidad de autenticación.

«Debido a la falta de autenticación en el portal de distribuidores locales, Indane filtra los nombres, las direcciones y los números de Aadhaar de sus clientes», escribió Robert en Medium.

Para evitar meterse en problemas con las autoridades indias, el investigador compartió sus hallazgos con Robert, quien anteriormente ganó fama por exponer numerosas filtraciones relacionadas con Aadhaar y debilidades de seguridad en otros sitios web y servicios de la India.

Luego de analizar el problema, Robert descubrió que los atacantes pueden obtener datos de millones de ciudadanos indios del sitio web de Indane si conocen el nombre de usuario de cada distribuidor, que luego descubrió que utiliza otra vulnerabilidad en la aplicación móvil oficial de Indane.

La vulnerabilidad de la app móvil le permitió a Robert encontrar 11,062 ID de distribuidor válidas, de las cuales utilizó 9490 ID en el portal de distribuidores en línea para obtener datos



personales de 5.8 millones de usuarios, incluidos sus números de Aadhaar, nombres y direcciones residenciales.

«Desafortunadamente, Indane probablemente bloqueó mi IP, por lo que no probé los 1572 distribuidores restantes. Al hacer algunos cálculos básicos, podemos estimar el número final de clientes afectados en cerca de 6,791,200», dijo Robert.

Robert compartió sus hallazgos con Indane, una marca de GLP propiedad de Indian Oil Corporation, el 15 de febrero, e hizo la divulgación pública el 19 de febrero luego de no recibir respuesta de la empresa.

Por su parte, Indian Oil Corp Ltd, propietaria de Indane, escribió en Twitter que *«No hay fugas de datos de Aadhaar por medio del sitio web de Indane»*.

En una declaración adjunta, en lugar de reconocer el incumplimiento de los datos de sus clientes, la compañía intentó defender a Aadhaar y al gobierno de la India diciendo:

«IndianOil en su software solo captura el número de Aadhaar que se requiere para la transferencia del subsidio de GLP. IndianOil no captura ningún otro detalle relacionado con Aadhaar. Por lo tanto, la filtración de datos de Aadhaar no es posible a través de nosotros».

«En el pasado, las compañías de comercialización de petróleo en forma periódica recibían el consumo de recargas de GLP subvencionadas por los consumidores, múltiples conexiones con información de clientes como número de consumidor, nombre, ID de GLP y dirección, en dominio público en sus sitios web respectivos que estaba disponible para auditorías sociales».



Compañía india de gas LPG filtró los datos de 6.7 millones de clientes

The Hacker News revisó la base de datos de muestra proporcionada por Robert y confirmó que el sitio web también alberga los números de Aadhaar de sus clientes, que no se muestran directamente en la página web, sino en la URL con hipervínculo a la ID de cada cliente.