Los investigadores de Check Point, Dikla Barda, Roman Zaikin y Yaara Shriki, revelaron hoy graves vulnerabilidades de seguridad en el asistente virtual Alexa de Amazon, que podrían causar una serie de ataques maliciosos.

Según el informe de Check Point Research, los *«exploits podrían haber permitido a un atacante eliminar/instalar habilidades en la cuenta de Alexa de la víctima objetivo, acceder a su historial de voz y adquirir información personal a través de la interacción de habilidades cuando el usuario invoca la habilidad instalada».*

> *«Los altavoces inteligentes y los asistentes virtuales son tan comunes que es fácil pasar por alto la cantidad de datos personales que tienen y su función en el control de otros dispositivos inteligentes en nuestros hogares»,* dijo Oded Vanunu, jefe de investigación de vulnerabilidades de productos.

Amazon corrigió las vulnerabilidades después de que los investigadores revelaron sus hallazgos a la compañías en junio de 2020.

Defecto XSS en uno de los subdominios de Amazon

Check Point dijo que las fallas se debían a una política CORS mal configurada en la aplicación móvil Alexa de Amazon, lo que potencialmente permite a los adversarios con capacidades de inyección de código en un subdominio de Amazon, realizar un ataque entre dominios en otro subdominio de Amazon.

La explotación exitosa requiere solo un clic en un enlace de Amazon que ha sido especialmente diseñado por el atacante, para dirigir a los usuarios a un subdominio de Amazon que es vulnerable a los ataques XSS.

Además, los investigadores encontraron que una solicitud para recuperar una lista de todas las habilidades instaladas en el dispositivo Alexa también devuelve un token CSRF en la

respuesta.

El propósito inicial de un token CSRF es evitar ataques de falsificación de solicitudes entre sitios en los que un enlace o programa malicioso hace que el navegador web de un usuario autenticado realice una acción no deseada en un sitio web legítimo.

Esto se debe a que el sitio no puede diferenciar entre solicitudes legítimas y solicitudes falsificadas.

Un mal actor con el token en posesión, puede crear solicitudes válidas al servidor backend y realizar acciones en nombre de la víctima, como instalar y habilitar una nueva habilidad para la víctima de forma remota.

El ataque funciona al pedir al usuario que haga clic en un enlace malicioso que navega a un subdominio de Amazon («track.amazon.com») con una falla XSS que se puede explotar para lograr la inyección de código.

Después, el atacante lo usa para activar una solicitud al subdominio «skillsstore.amazon.com», con las credenciales de la víctima para obtener una lista de todas las habilidades instaladas en la cuenta de Alexa y el token CSRF.

En la etapa final, el exploit captura el token CSRF de la respuesta y lo utiliza para instalar una habilidad con una ID de habilidad específica en la cuenta de Alexa del objetivo, eliminar sigilosamente una habilidad instalada, obtener el historial de comandos de voz de la víctima e incluso acceder a la información personal almacenada en le perfil del usuario.

Se espera que el tamaño del mercado global de altavoces inteligentes alcance los 15.6 mil millones de dólares para 2025, por lo que la seguridad es un tema muy importante para dispositivos IoT.

> *«Los dispositivos de IoT son inherentemente vulnerables y aún carecen de la*

> *seguridad adecuada, lo que los convierte en objetivos atractivos para los actores de amenazas»,* dijeron los investigadores.
>
> *«Los ciberdelincuentes buscan continuamente nuevas formas de violar los dispositivos o utilizarlos para infectar otros sistemas críticos. Tanto el puente como los dispositivos sirven como puntos de entrada. Deben mantenerse seguros en todo momento para evitar que los hackers se infiltren en nuestros hogares inteligentes».*