PERÚ | Presidencia del Consejo de Ministros | Secretaría de Gobierno y Transformación Digital

ALERTA INTEGRADA DE SEGURIDAD DIGITAL

Asociación de Bancos del Perú

ALERTA INTEGRADA DE SEGURIDAD DIGITAL

225-2024-CNSD

La presente **Alerta Integrada de Seguridad Digital** corresponde a un análisis técnico periódico realizado por el Comando Conjunto de las Fuerzas Armadas, el Ejército del Perú, la Marina de Guerra del Perú, la Fuerza Aéreadel Perú, la Dirección Nacional de Inteligencia, la Policía Nacional del Perú, la Asociación de Bancos del Perú y el Centro Nacional de Seguridad Digital de la Secretaría de Gobierno y Transformación Digital de la Presidencia del Consejo de Ministros, en el marco de la Seguridad Digital del Estado Peruano.

El objetivo de esta alerta **es informar a los responsables de la seguridad digital de las entidades públicas y lasempresas privadas sobre las amenazas en el entorno digital** para advertir las situaciones que pudieran afectar la continuidad de sus servicios en favor de la población.

Las marcas y logotipos de empresas privadas y/o entidades públicas se reflejan para ilustrar la información que los ciudadanos reciben por redes sociales u otros medios y que atentan contra la confianza digital de las personas y de las mismas empresas **de acuerdo con lo establecido por el Decreto de Urgencia 007-2020**.

La presente Alerta Integrada de Seguridad Digital es información netamente especializada para informar a las áreas técnicas de entidades y empresas.

Contenido

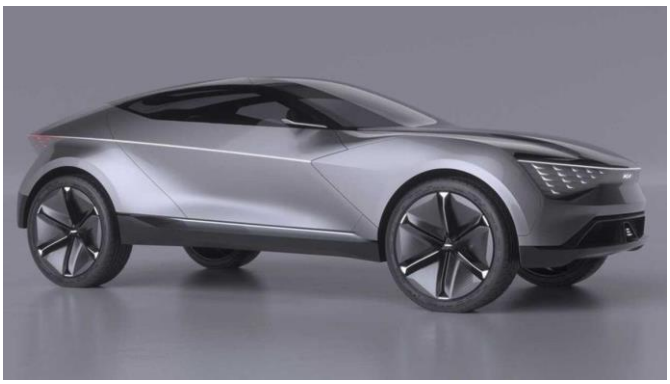
Centro Nacional de Seguridad Digital	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N°225	Fecha: 28-09-2024
		Página: 4 de 6

Componente que reporta	CENTRO NACIONAL DE SEGURIDAD DIGITAL		
Nombre de la alerta	Los piratas informáticos podrían controlar de forma remota los coches Kia aprovechando las matrículas		
Tipo de Ataque	Explotación de vulnerabilidades conocidas	Abreviatura	EVC
Medios de propagación	Red, Internet		
Código de familia	H	Código de Sub familia	H01
Clasificación temática familia	Intento de intrusión		

Descripción

1. ANTECEDENTES:

Los investigadores de seguridad Neiko Rivera, Sam Curry, Justin Rhinehart e Ian Carroll descubrieron un conjunto de vulnerabilidades que podrían haber sido explotadas para obtener acceso no autorizado a los vehículos Kia mediante el uso de la infraestructura del concesionario Kia, para aquellos automóviles fabricados después del 2013 utilizando solo la matrícula del vehículo en cuestión.



2. DETALLES:

Hace casi dos años, en 2022, algunos de los piratas informáticos de este grupo, incluido el investigador de seguridad y cazador de errores Sam Curry, encontraron otras vulnerabilidades críticas que afectaban a más de una docena de empresas automotrices y que habrían permitido a los delincuentes localizar, desactivar los arrancadores, desbloquear y arrancar de forma remota más de 15 millones de vehículos fabricados por Ferrari, BMW, Rolls Royce, Porsche y otros fabricantes de automóviles.

Curry reveló que las vulnerabilidades del portal web de Kia descubiertas el 11 de junio de 2024 podrían explotarse para controlar cualquier vehículo Kia equipado con hardware remoto en menos de 30 segundos, "independientemente de si tenía una suscripción activa a Kia Connect".

El ataque implicó que los atacantes se registraran de forma remota para obtener una cuenta falsa y generaran tokens de acceso. Estos tokens luego se usarían junto con otra solicitud HTTP a un punto final APIGW (API Gateway) del concesionario y el VIN (número de identificación del vehículo) del vehículo para obtener el nombre, el número de teléfono y la dirección de correo electrónico del propietario, y potencialmente agregarse como un segundo usuario "invisible" en el automóvil sin el conocimiento del propietario.

Los investigadores descubrieron que se podía acceder al vehículo de una víctima ejecutando cuatro solicitudes HTTP y comandos de Internet al vehículo:

- Generar un token de distribuidor y recuperarlo de la respuesta HTTP
- Acceda a la dirección de correo electrónico y al número de teléfono de la víctima.
- Modificar los permisos de acceso del propietario utilizando información filtrada.
- Agregar un correo electrónico controlado por el atacante al vehículo de la víctima, lo que permite comandos remotos.

La víctima no recibiría ninguna notificación sobre las modificaciones de sus permisos de acceso.

Las funcionalidades vulnerables son las siguientes:

- Bloqueo/desbloqueo remoto: pueden bloquear o desbloquear las puertas.
- Geolocalizar el vehículo: los hackers podrían determinar la ubicación del coche.
- Arranque/parada remota: Podrían arrancar o apagar el motor de forma remota.
- Bocina/Luz remota: Podrían activar la bocina y las luces del auto.
- Cámara remota: En algunos casos, incluso podrían acceder a las cámaras del automóvil.

Vehículos afectados:

El fallo afectó a varios modelos de Kia a lo largo de distintos años de fabricación. Entre los vehículos afectados se encuentran las versiones 2025 del Carnival EX, SX, LX y Hybrid, así como los modelos K5 y Sportage.

Modelos afectados:

- 2025 Carnival EX, SX, LX y Hybrid
- 2025 K5
- 2025 Sportage

Los ataques permitieron a los hackers no solo controlar funciones básicas del vehículo, sino también acceder a información privada de los dueños, sin que estos se dieran cuenta.

Las implicaciones de este fallo pueden ser graves, ya que un atacante podía tomar control efectivo de un vehículo sin el conocimiento o consentimiento del propietario. La capacidad de rastrear vehículos y emitir comandos remotos representaba riesgos significativos para la privacidad y la seguridad de los conductores. Además, este tipo de vulnerabilidad pone de relieve las crecientes amenazas a las que se enfrentan los vehículos conectados y cómo la industria automotriz debe adaptarse rápidamente a estos desafíos.

Tras el descubrimiento de la vulnerabilidad, los investigadores reportaron el problema a Kia, que implementó rápidamente soluciones para corregir los fallos de seguridad. Kia confirmó que no había evidencia de explotación maliciosa de estas vulnerabilidades antes de que fueran parcheadas.

A medida que los vehículos se vuelven cada vez más conectados y dependientes de sistemas digitales, es crucial garantizar medidas de ciberseguridad robustas. Los fabricantes deben priorizar la seguridad en sus procesos de diseño y mantenerse vigilantes ante las amenazas emergentes.

3. RECOMENDACIÓN:

- Permanecer alertas a los posibles descubrimientos de nuevas vulnerabilidades. Actualmente el proveedor ya lo ha solucionado.

Fuente de Información:	• hxxps://www.bleepingcomputer.com/news/security/kia-dealer-portal-flaw-could-let-attackers-hack-millions-of-cars/ • hxxps://hackread.com/hackers-control-kia-cars-exploiting-license-plates/ • hxxps://bitlifemedia.com/2024/09/un-fallo-en-una-web-de-kia-permite-controlar-vehiculos-remotamente-usando-solo-la-matricula/

Índice alfabético