	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N° 085	**Fecha: 11-04-2023**
		Página 11 de 43

Componente que reporta	**CENTRO DE CIBERDEFENSA DEL EJÉRCITO DEL PERÚ**		
Nombre de la alerta	Dos vulnerabilidades de 0 días explotadas activamente para piratear iphones y ipads		
Tipo de ataque	Malware	Abreviatura	Malware
Medios de propagación	Redes sociales, SMS, correo electrónico, videos de internet, entre otros		
Código de familia	C	Código de subfamilia	C02
Clasificación temática familia	Código malicioso		

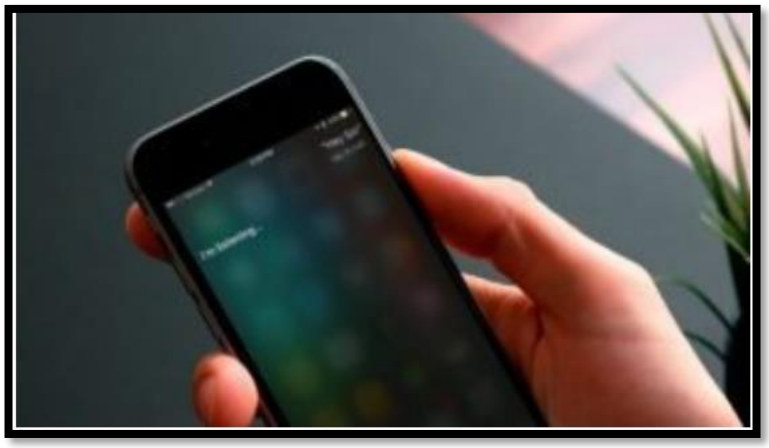
Descripción

ANTECEDENTES:

El 07 de abril del 2023, a través del monitoreo y búsqueda de amenazas en el Ciberespacio, se descubrió que, Apple los consumidores han recibido un golpe en un mundo donde la seguridad digital es de suma importancia debido a la reciente revelación de dos vulnerabilidades de día cero que afectan a una variedad de dispositivos. Los investigadores Clément Lecigne del Grupo de Análisis de Amenazas de Google y Donncha o Cearbhaill del Laboratorio de Seguridad de Amnistía Internacional fueron los que encontraron las vulnerabilidades, a los que se les han dado los identificadores CVE-2023-28205 y CVE-2023-28206. Ambas vulnerabilidades han sido explotadas activamente, lo que aumenta las apuestas para los consumidores y pone a Apple en alerta máxima.

DETALLES:

La vulnerabilidad sin uso conocida como CVE-2023-28205 se descubrió en WebKit**:** Es la primera vulnerabilidad que discutir. Es posible explotarlo engañando a objetivos para cargar páginas web maliciosas bajo el control de atacantes, lo que puede resultar en la ejecución de malware en computadoras que han sido infiltradas. Visitar un sitio web que se ha infiltrado es todo lo que se necesita para que los piratas informáticos tomen el control de su dispositivo, para ponerlo en palabras de laicos.



El procesamiento de material en línea que ha sido diseñado maliciosamente tiene el potencial de resultar en la ejecución de código arbitrario, lo que otorga a los atacantes acceso no autorizado a su dispositivo.

Vulnerabilidad de escritura fuera de límites del acelerador IOSurface, también conocida por su número CVE 2023-28206:

La segunda falla, identificada como CVE-2023-28206, es un problema de escritura que ocurre cuando se exceden los límites de IOSurfaceAccelerator. Esta vulnerabilidad puede ser explotada por una aplicación para ejecutar código arbitrario con privilegios de kernel, lo que brinda a los atacantes el máximo grado de acceso posible al dispositivo de destino.

Si una aplicación aprovecha esta vulnerabilidad, puede ejecutar código arbitrario mientras mantiene los privilegios del núcleo. Esto efectivamente les daría a los atacantes el control del dispositivo que está utilizando. Al fortalecer la validación de entrada, Apple ha solucionado el problema de escritura fuera de límites que existía anteriormente.

La empresa emitió actualizaciones críticas de seguridad en febrero para abordar una vulnerabilidad de día cero explotada activamente que se rastreó como CVE-2023-23529 y afecta a iOS, iPadOS y macOS.

La vulnerabilidad de seguridad, que es un problema de confusión de tipos en WebKit, fue fijada por el gigante tecnológico mediante la implementación de verificaciones mejoradas.

Al manipular a las víctimas para que accedan a contenido en línea maliciosamente diseñado, un atacante puede realizar la ejecución arbitraria de código y tomar el control del sistema de la víctima.

Apple ha confirmado que una gran cantidad de productos están incluidos en la lista de los afectados. Esto incluye lo siguiente:

iPhone8 y modelos posteriores, iPad Pro todos los modelos, modelos iPad Air que comienzan con los modelos iPad de tercera generación y posteriores, comenzando con la quinta generación y más tarde, modelos iPad mini que comienzan con la quinta generación y más tarde, y Macs ejecutando macOS Vista.

RECOMENDACIONES:

- Actualizar rápidamente sus dispositivos para evitar la posibilidad de ser explotados.
- Mantener un enfoque proactivo de la ciberseguridad y mantener todos sus dispositivos actualizados con los parches y actualizaciones de software más recientes.

Fuentes de información	▪ hxxps://www.securitynewspaper.com/2023/04/07/two-actively-exploited-0-day-vulnerabilities-can-be-used-to-hack-iphones-and-ipads/