Nro. Alerta:	EC-2022-005	CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS DEL ECUADOR **ALERTAS DE SEGURIDAD**	CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS ECUCERT
TLP:	TLP:BLANCO		
Fecha:	05-enero-2022	**Apple iOS: error de programa en "HomeKit DoorLock" podría generar denegación de servicio**	V 1.0

I. DATOS GENERALES:

Clase de alerta: Vulnerabilidad

Tipo de incidente: Sistema vulnerable

Nivel de riesgo: Medio

II. ALERTA

Vulnerabilidad persistente de denegación de servicio (DoS) en el sistema operativo móvil iOS de Apple, es capaz de forzar a dispositivos afectados, a un ciclo de bloqueo o reinicio al conectarse a un dispositivo compatible con Apple Home.

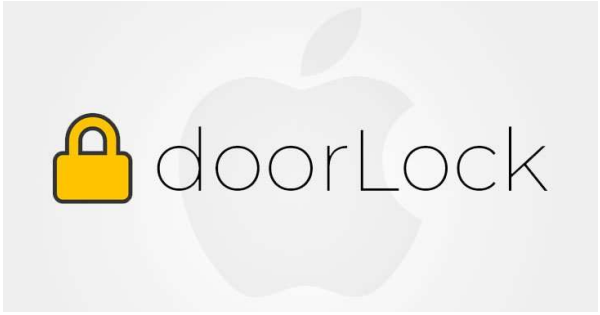

Figura 1. Door Lock de iOS **Fuente:** TheHackerNews

III. INTRODUCCIÓN

HomeKit, es el Software de Apple que permite a usuarios de iOS y iPadOS, configurar, comunicarse y controlar accesorios conectados y electrodomésticos inteligentes utilizando dispositivos Apple, éste software, presenta un error en el sistema, el cual se informó inicialmente el 10 de agosto de 2021, sin embargo, permanece en iOS 15.2. Apple declaró que planeaba resolver el error en una actualización de seguridad antes de 2022, pero hasta la presente fecha, no existe una solución real. Se han probado todas las versiones de iOS lanzadas desde iOS 14.7 y la vulnerabilidad existe en todas las versiones.

Los dispositivos utilizados durante las pruebas de concepto y posterior explotación de este

bug, incluyen un iPhone 7 (iOS 15.2-14.7), un iPad 6 (iOS 15.0 beta e iOS 14.7) y un iPhone XS (iOS 14.7.1 y 14.7). Si bien no se ha probado, es probable que el error exista en todas las versiones de iOS 14.

La descripción general del error (bug) en el sistema iOS es la siguiente: cuando el nombre de un dispositivo HomeKit se cambia a una cadena grande (500,000 caracteres en la prueba de concepto), cualquier dispositivo con una versión de iOS afectada instalada, que cargue la cadena, se interrumpirá, incluso después de reiniciar.

Restaurar un dispositivo y volver a iniciar sesión en la cuenta de iCloud vinculada al dispositivo HomeKit, volverá a desencadenar el error.

IV. VECTOR DE ATAQUE

Local (probado inicialmente) y Red (posibilidad de escalamiento)

V. IMPACTO:

En un escenario de ataque del mundo real, un atacante podría aprovechar el bug de "DoorLock" enviando una invitación maliciosa para conectarse a un dispositivo HomeKit con una cadena anormalmente grande como su nombre, bloqueando efectivamente a los usuarios de sus datos locales y evitando que vuelvan a iniciar sesión iCloud en iOS.

Dado que los nombres de los dispositivos HomeKit también se almacenan en iCloud, iniciar sesión en la misma cuenta de iCloud con un dispositivo restaurado, activará el bloqueo una vez más, a menos que el propietario del dispositivo opte por desactivar la opción para sincronizar los datos de HomeKit.

Este problema, hace que el ransomware sea viable para iOS, lo cual es increíblemente significativo. Las aplicaciones con acceso a los datos de inicio de los propietarios de dispositivos HomeKit pueden bloquear al usuario de sus datos locales y, evitar que vuelvan a iniciar sesión en su iCloud en iOS, según la versión de iOS. Un atacante también podría enviar invitaciones a un hogar que contenga los datos maliciosos a los usuarios en cualquiera de las versiones de iOS descritas, incluso si no tienen un dispositivo HomeKit.

Un atacante podría usar direcciones de correo electrónico que se parezcan a los servicios de Apple, o los productos HomeKit, para engañar a usuarios menos expertos en tecnología

Nro. Alerta:	EC-2022-005	CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS DEL ECUADOR **ALERTAS DE SEGURIDAD**	CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS ECUCERT
TLP:	TLP:BLANCO		
Fecha:	05-enero-2022	**Apple iOS: error de programa en "HomeKit DoorLock" podría generar denegación de servicio**	V 1.0

(o incluso a aquellos que tienen curiosidad), para que acepten la invitación y luego exijan el pago por correo electrónico a cambio de solucionar el problema.

No se ha identificado un método confiable para recuperar el acceso a los datos locales después de que se haya desencadenado el error (bug)

VI. RECOMENDACIONES

El EcuCERT recomienda a su comunidad objetivo tomar en consideración lo siguiente:

- Restaurar el dispositivo afectado desde el modo de recuperación o DFU
- Configurar el dispositivo como de costumbre, pero no vuelva a iniciar sesión en la cuenta de iCloud en primera instancia hasta finalizar la configuración.
- Una vez finalizada la configuración, inicie sesión en iCloud desde la configuración. Inmediatamente después de hacerlo, desactive el interruptor etiquetado como "Inicio". El dispositivo y iCloud ahora deberían funcionar nuevamente sin acceso a los datos de Inicio.
- Descargar aplicaciones, documentos, y en sí, archivos de cualquier naturaleza, solo desde fuentes oficiales y legítimas.
- No abrir, manipular, o interactuar con correos electrónicos altamente sospechosos recibidos en las respectivas bandejas de correo ya sea personales o Institucionales.
- En el caso de sufrir un ataque de proporciones mayores, contacte a las Autoridades competentes en base a la Normativa Legal Vigente a nivel Nacional.

VII. REFERENCIAS:

Ravie Lakshmanan. (4 de enero de 2022). TheHackerNews. Obtenido de https://thehackernews.com/2022/01/researchers-detail-new-homekit-doorlock.html

Trevor Spiniolas. (1 de enero de 2022). Trevor Spiniolas. Obtenido de https://trevorspiniolas.com/doorlock/doorlock.html