RESPUESTA DEL GOBIERNO

(184) PREGUNTA ESCRITA CONGRESO

184/18251 **17/10/2017** **51250**

AUTOR/A: TEN OLIVER, Vicente (GCS)

RESPUESTA:

En relación con el asunto interesado, se señala que la vulnerabilidad en el protocolo WPA2 descubierta por los investigadores de la Universidad de Lovaina ha sido confirmado por los principales fabricantes de sistemas operativos que integran tecnologías Wi-Fi. Muchos de ellos han publicado diferentes parches para corregir esta vulnerabilidad, ya que han podido corroborar la existencia de la misma en algunos de sus productos.

La organización que se asegura de la interoperabilidad de los dispositivos inalámbricos entre diferentes fabricantes, Wi-Fi Alliance, también ha podido corroborar esta información y proporciona a los fabricantes de dispositivos inalámbricos una herramienta de detección en sus laboratorios, así como los detalles técnicos necesarios para el desarrollo de parches.

También desde el CERT/CC (CERT Coordination Center), el equipo de respuesta a incidentes informáticos creado por la Universidad Carnegie Mellon, CERT pionero y precursor de otros CERT a nivel mundial, y al que estos investigadores comunicaron y proporcionaron los detalles técnicos, ha podido corroborar esta información, documentándola y alertando a los posibles afectados.

Por ello, el Gobierno puede confiar en los descubrimientos técnicos realizados por los investigadores que han analizado la seguridad del protocolo WPA2 utilizado en redes inalámbricas Wi-Fi.

Desde el Gobierno y en concreto desde el Instituto Nacional de Ciberseguridad (INCIBE), organismo dependiente del Ministerio de Energía, Turismo y Agenda Digital a través de la Secretaría de Estado para la Sociedad de la Información y Agenda Digital, se están realizando acciones para ello desde el mismo día 16 de octubre en el que fueron publicadas las vulnerabilidades descubiertas en el protocolo WPA2.

Concretamente, en relación con este hallazgo, y con carácter de alerta temprana, el mismo día 16 se elaboraron, publicaron y difundieron distintos avisos, alertas y boletines de ciberseguridad para diferentes públicos interesados:

1. Ciudadanos:https://www.osi.es/es/actualidad/avisos/2017/10/routers-wifi-vulnerables-han-conseguido-romper-el-protocolo-de-seguridad
2. Empresas: https://www.incibe.es/protege-tu-empresa/avisos-seguridad/importante-fallo-el-protocolo-wpa2-pone-riesgo-seguridad-las
3. Profesionales de la ciberseguridad: https://www.certsi.es/alerta-temprana/avisos-seguridad/importante-vulnerabilidad-wpa2

Adicionalmente, se difundieron estas alertas a través de los diferentes canales de redes sociales de INCIBE para hacer llegar los avisos lo más dinámicamente posible.

Además, con carácter específico, los operadores estratégicos fueron objeto de una comunicación especial informando dicho hallazgo por su especial componente.

Las labores de comunicación, formación, concienciación y desarrollo de nuevas herramientas tecnológicas para garantizar la seguridad y privacidad en el uso de los servicios de la Sociedad de la Información en general son lideradas desde equipos de respuesta a incidentes (CERT – Computer Emergency Response Team) como es, en el caso de España, INCIBE. La generalización de la digitalización de los servicios y de la sociedad en general hace de la ciberseguridad un reto que requiere tratamiento y esfuerzo continuo que ha de venir necesariamente acompañado del respaldo político y económico proporcional. Ejemplo de la importancia de estas acciones es la propia evolución de INCIBE que en el año 2017 ha recibido el mayor presupuesto desde su creación.

Madrid, 17 de abril de 2018