https://politica.elpais.com/politica/2017/11/09/actualidad/1510217634_470836.html

La policía desactiva la firma digital del DNI por fallos de seguridad

La vulnerabilidad ha sido descubierta por una universidad checa y afecta a los expedidos desde 2015

Aitor Bengoa

Madrid 9 NOV 2017 - 22:33 CET

Imágenes del DNI facilitadas por la policía.

La función de certificado digital de los DNI electrónicos expedidos desde abril de 2015 ha sido desactivada por la Policía después de que un estudio de una universidad checa haya alertado de un posible fallo de seguridad de este sistema de identificación *online,* que permite hacer diversos trámites administrativos, mercantiles y privados.

MÁS INFORMACIÓN

-  Un mes y medio para sacarse el DNI
- Más de 2.000 personas han cambiado su sexo en el DNI desde 2007

La vulnerabilidad fue descubierta en enero de este año por el equipo del profesor Petr Svenda, del Centro para la Investigación de Criptografía y Seguridad vinculado a la

Universidad Masaryk. “En las tarjetas hay un pequeño chip que contiene dos códigos, uno público y otro privado. Ambos están conectados, pero el privado nunca debería salir del chip”, explica Svenda por teléfono a EL PAÍS. “La vulnerabilidad, conocida como ROCA, consiste en que la parte pública contiene información suficiente para que, mediante un proceso conocido como factorización, se pueda descifrar el código privado”, detalla. Así, un *hacker* con los medios necesarios podría suplantar al dueño del chip.

Fuentes policiales consultadas por este periódico confirman que ese fallo afecta a los DNI, pero remarcan que se trata de una “supuesta vulnerabilidad teórica” que proviene de un estudio universitario y que “no se ha llegado a explotar en la práctica”. Es decir, que no se han detectado casos de que nadie se haya aprovechado del fallo. Países como Estonia o Eslovaquia también se han visto afectados, según Svenda, que asegura que su equipo avisó a la empresa alemana que fabrica los chips en febrero e hizo públicos los resultados del estudio hace una semana. “Se supone que la empresa avisaría a sus clientes”. Sin embargo, fuentes policiales señalan que no han recibido ninguna advertencia.

Porcentaje muy pequeño

Las mismas fuentes aclaran que el porcentaje de DNI que podrían verse afectados “es residual”. Esto se debe a que solo los expedidos después de abril de 2015 estarían expuestos. Además, para que en teoría fueran vulnerables primero habría que activarlos y llegar a usarlos, y el porcentaje de DNI que cumplen estos supuestos es muy pequeño. La desactivación ha sido adoptada con carácter preventivo "con el objetivo de mejorar su seguridad para evitar cualquier tipo de vulnerabilidad en el futuro” y garantizar la seguridad y confidencialidad de los usuarios.

Svenda plantea dos soluciones: modificar el código o cambiar el algoritmo en el que se basa el proceso de certificación. Sin embargo, de cara a elevar la seguridad a un nivel mayor, cree que la mejor opción sería fragmentar el código para que una parte estuviera almacenada en otro dispositivo, como el teléfono móvil. De este modo, un hacker tendría que atacar dos dispositivos en lugar de uno para descifrarlo.

"Este problema no es nuevo, hace diez años que existía, pero no había sido detectado", comenta el investigador checo. Para este experto, este tipo de fallos de seguridad podrían identificarse mucho antes y con más facilidad si hubiera más transparencia, ya que las empresas "guardan en secreto los procesos de certificación y de generación de algoritmos". "Si los datos fueran públicos, todo el mundo podría revisarlos y encontrar fallos", asegura.

LOS EXPEDIDOS A PARTIR DE ABRIL DE 2015

Los DNI que pueden verse afectados por la vulnerabilidad ROCA son los que tienen el número de soporte posterior al ASG160.000, expedidos a partir de abril de 2015. La solución a este fallo de seguridad está ya "prácticamente definida", según fuentes policiales. Cuando se ponga en marcha, se informará a los titulares para que actualicen las firmas digitales en las oficinas de documentación. Mientras, siguen siendo válidos como documento de identificación para cualquier tipo de trámite y y como documento de viaje para viajar a los países de la UE.