proactive
Information security.

Ayudamos a Proteger sus Activos de Información

ProActive News Vol.4

Setiembre 2017

Equifax Data Breach & Blueborne

Equifax, es una empresa global de reporte y scoring de crédito con sede en Atlanta, Georgia (USA) y que opera en el mercado local (adquirió a la empresa Informconf en el año 2013), reporto el día 7 de setiembre que su Casa Matriz en Estados Unidos sufrió un acceso no autorizado a sus sistemas (*data breach*) en el cual los intrusos probablemente pudieron tener acceso a información personal (nombres, fechas de nacimiento, números de seguridad social, direcciones de correo electrónico, entre otras) de 143 millones de clientes.

Técnicamente, lo que se maneja es que la intrusión pudo haberse debido a una vulnerabilidad en el software ***Struts*** de la fundación Apache, el cual es un *framework* para el desarrollo de aplicaciones web bajo la plataforma Java para empresas, más conocida como J2EE, la cual fue una tecnología pionera en su momento (año 2000) y razón por la que las empresas que la implementaron en su momento, la siguen utilizando hasta la actualidad.

La fundación Apache se pronunció al respecto en un comunicado que podemos resumir en: "*si utilizas un sistema y la empresa responsable del mismo ha emitido un parche de seguridad, parchea tu sistema*". Algo muy básico en seguridad, pero que a veces no es tan fácil de realizar, pero que lastimosamente volvemos a repetir e insistir: **Actualicen sus sistemas a los últimos publicados por el fabricante**.

Referencias:

- https://www.equifaxsecurity2017.com
- https://blogs.apache.org/foundation/entry/apache-struts-statement-on-equifax

Una visión más técnica y el exploit disponible:

- https://github.com/mazen160/struts-pwn_CVE-2017-9805

Blueborne es un conjunto de vulnerabilidades publicadas responsablemente por la empresa de seguridad Armis, que afecta a la implementación del protocolo Bluetooth .... con logotipo incluido.

Volvemos al caso anterior, actualización de sistemas. Windows y Linux ya han publicado parches se seguridad para solucionar esta vulnerabilidad. Apple, manifestó que sus sistemas no son vulnerables en su última versión, pero la parte más afectada es el sistema operativo para Smartphones Android, pues aunque la versión oficial de esta plataforma ya se encuentra corregida, la diversidad del ecosistema y fabricantes disponibles, sumado al tiempo en que tardan en publicar una actualización, crean bastante preocupación al respecto. El panorama más sombrío aún está en el ámbito de Internet de las Cosas (IoT), cuya actualización por parte de los fabricantes es muy escasa o nula.

Para resumir a que estamos expuestos: El ataque no requiere que la víctima interactúe con el dispositivo atacante. Esto quiere decir que pueden tomar el control de tu dispositivo sin necesidad de que te conectes a ningún sitio concreto con él. Los investigadores que han descubierto este fallo ya se han puesto en contacto con los fabricantes afectados, por lo que aunque se calcule que haya alrededor de 5.000 millones de dispositivos vulnerables las soluciones para la mayoría de ellos no deberían tardar en llegar.

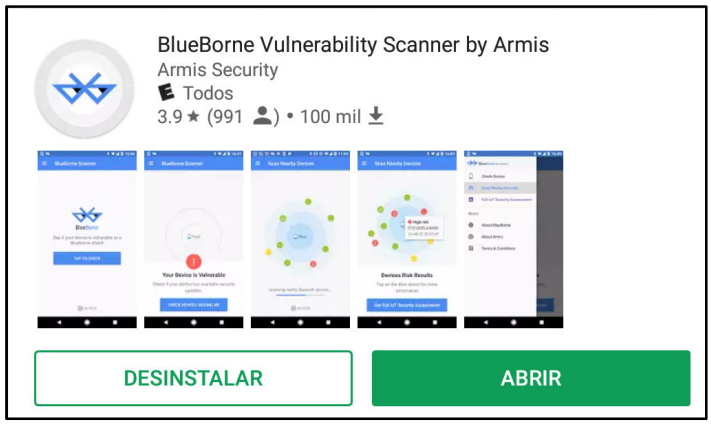
Simplemente vale con que tengas activado el Bluetooth para que un atacante pueda conectarse a tu dispositivo sin que te des cuenta a infectarlo con el malware que desee. Esto quiere decir que un dispositivo infectado con BlueBorne puede infectar a otro que tenga habilitado el Bluetooth a su alrededor, y que incluso una vez infectados estos dispositivos pueden propagar a su vez el malware.

En las pruebas internas realizadas por el grupo de investigación que descubrió la vulnerabilidad consiguieron tomar el control de dispositivos Android como los Google Pixel, Samsung Galaxy, Galaxy

Tab, LG Watch Sport, también en otros dispositivos Linux como los Samsung Gear 3 o Smart TV de Samsung, todos los iPhone, iPad e iPod Touch con iOS 9.3.5 en adelante y dispositivos AppleTV con su versión 7.2.2. Además lo han probado con éxito en ordenadores con versiones de Windows a partir de Windows Vista, y con todos los dispositivos GNU/Linux a partir de la versión 3.3-rc1 del Kernel lanzada en octubre del 2011.

Mientras llega la inminente próxima actualización de seguridad deberías extremar las precauciones y estar atento a tu dispositivo, o mantener apagado el bluetooth.

Puedes comprobar si tu dispositivo es vulnerable instalando la app de Armis desde Google Play.



Referencias:

- https://youtu.be/LLNtZKpL0P8
- https://youtu.be/Az-190RCns8

Con objeto de mantenerlo actualizado y protegido, quedamos a vuestra disposición para asesorarlo en cuanto a la detección de vulnerabilidades en su plataforma que puedan ser explotadas.

Obtenga mayor información sobre nuestros servicios y productos, póngase en contacto con nosotros:

Web: www.proactive.consulting

Mail: contacto@proactive.consulting

Tel: +595 (981) 478-921

Twitter: @ProActive_py