UT01: Adopción de pautas de seguridad informática - Vulnerabilidades

Nombre: Francisco Jesús García – Uceda Díaz - Albo
Curso: 2º ASIR.

Índice

a) Realiza un breve informe sobre vulnerabilidades actuales detectas en aplicaciones y sistemas operativos como Windows, Linux, Apple, Android, Wireless, Chrome etc.

Las vulnerabilidades están presentes en todos lados hoy en día, veremos cómo en este breve informe hablamos sobre vulnerabilidades en los sistemas y aplicaciones del gigante Microsoft, como hay vulnerabilidades a nivel de hardware en los procesadores o incluso en el sistema operativo de la gigante Apple o en las mismas tarjetas SIM.

Empecemos por el gigante Microsoft y el cual es muy conocido por las polémicas actualizaciones y brechas de seguridad que se encuentran. Hablemos de la vulnerabilidad encontrada identificada CVE-2019-1255. Esta afecta a antivirus de Microsoft conocido como Windows Defender. Se trata de una vulnerabilidad de denegación de servicio que puede ser explotada por un atacante para impedir la ejecución de binarios legítimos del sistema. A día de hoy (24 de septiembre de 2019), la vulnerabilidad ha sido corregida por el equipo de Microsoft, pero claro, no todos los equipos están actualizados.

Seguimos en Microsoft y nos encontramos con el navegador de Microsoft, lo que parecía ser un gran avance para Microsoft ha supuesto un dolor de cabeza para estos. Esta vulnerabilidad clasificada como grave, permite la ejecución remota de código aprovechando la forma en que el motor de scripting maneja los objetos de la memoria en Internet Explorer. El fallo podría corromper la memoria de tal manera que un atacante puede ejecutar código arbitrario y obtener los mismos privilegios de usuario que el usuario actual. Los parches han sido emitidos desde el equipo de Microsoft, aunque volvemos a lo mismo, si la gente no actualiza la vulnerabilidad no es corregida.

Continuando con el informe (y siguiendo con sistemas operativos) nos vamos a los dos mayores sistemas operativos para móviles, Android e IOS. Siempre se ha dicho que IOS no tenía vulnerabilidades y esto es mentira como desvela este último informe sacado, o eso es lo que destaca la conocida firma ESET en lo que revela que en este 2019 han aumentado un 25% las vulnerabilidades del sistema operativo IOS (respecto a 2018) y casi el doble respecto al sistema operativo de Google, Android. Durante el Q1 (primer trimestre) el 43% de esas vulnerabilidades se concentraron en China.

Increíblemente y aunque pueda parecer mentira, ESET revela también un dato más que curioso, y es que en lo que va de año respecto a 2018 las vulnerabilidades críticas en Android bajaron un 20%, aunque eso sí, la firma destaca que 9 de 10 dispositivos Android funciona con versiones anteriores a Android Pie (9.0) por lo cual esto los hacen vulnerables por los problemas de seguridad que representa.

Continuando con vulnerabilidades en software nos vamos a otra aplicación de Google, el Google Chrome, y es que se han encontrado nada menos que cuatro vulnerabilidades catalogadas como crítica en este navegador el cual aún no han sido parchedas.

En el caso de la vulnerabilidad crítica (CVE-2019-13685), la misma fue reportada el 5 de septiembre por Khalil Zhani y permitiría a un atacante tomar el control de un equipo infectado de manera remota. Las otras tres son la CVE-2019-13688, CVE-2019-13687 y CVE-2019-13686. Las dos primeras reportadas por Man Yue Mo, mientras que Brendon Tiszka hizo lo propio con la tercera.

Según explicó la compañía en un comunicado, los detalles de estas vulnerabilidades permanecerán en secreto hasta se encuentre una solución y la mayoría de usuarios actualicen a la última versión del navegador cuando se haya lanzado el parche correspondiente para cada una de ellas.

Según informes previos, la explotación de estas vulnerabilidades permitiría a un atacante ejecutar código de manera arbitraria en el contexto del navegador. Lo único que necesitaría el atacante es lograr que la víctima abra un sitio web especialmente diseñado en el navegador, sin necesidad de que interactúe de manera adicional con el sitio.

Para continuar y al mismo tiempo finalizar con el informe nos iremos a las peores vulnerabilidades posibles (no, no hablo de 0 days), las que ocurren a nivel de hardware y son muy muy difíciles de mitigar.

Nos vamos a las tarjetas SIM las cuales se ha dado a conocer una vulnerabilidad bautizada como Simjacker, esta te permite ver la localización del usuario en todo momento.

Esta está catalogada como crítica ya que afecta a todos los dispositivos que usen tarjeta SIM. El ataque comienza con un SMS formateado con una "especie de código spyware" que contiene órdenes para la UICC (siglas de "Universal Integrated Circuit Card" y más conocida comúnmente como tarjeta SIM). Dichas órdenes se pueden ejecutar explotando S@T Browser, una parte del sistema operativo de las tarjetas SIM antiguas. S@T Browser ya no se usa, pero sigue presente en las tarjetas SIM de más de mil millones de usuarios a nivel global. Cuando se ejecuta el código, este recopila información de la tarjeta SIM como nuestra ubicación o el número IMEI para, posteriormente, mandarlo como SMS al atacante, todo esto siempre en segundo plano y sin ningún tipo de conocimiento por parte del usuario.

Pero no solo puede recabar esa información, sino que Simjacker permite reproducir sonido, apagar la tarjeta, lanzar el navegador, enviar datos, enviar mensajes multimedia o SMS... Así, se convierte en una vulnerabilidad que podría usarse para varios fines, desde fraude y suplantación de identidad hasta espionaje.

Para finalizar el informe hablaremos de algo más escalofriante, y es de las vulnerabilidades de los procesadores a nivel de hardware. Los procesadores de Intel se han mostrado como los más inseguros probablemente de la historia. Todos los procesadores de la gama Core están expuestos

ya a más de una decena de vulnerabilidades, la mayoría relacionados con la ejecución especulativa. Ahora, un nuevo fallo llamado NetCAT afecta a los procesadores más potentes de la marca.

Los procesadores Intel Xeon pueden filtrar contraseñas y datos confidenciales por esta vulnerabilidad, algo escalofriante sabiendo que estos procesadores se usan en empresas y CPD de alto rendimiento. Parchear esta vulnerabilidad no solo es complicado si no, que se pierde un gran rendimiento a todos los procesadores Xeon desde 2011. Intel incluyó una función que mejoraba el rendimiento en los servidores permitiendo que las tarjetas de red y otros periféricos se conectasen directamente a la memoria caché de la CPU en lugar de hacerlo a la memoria RAM del ordenador como se ha hecho siempre.

Este sistema, llamado DDIO, mejora el ancho de banda, además de reducir la latencia y el consumo energético. Unos investigadores han descubierto que un atacante puede aprovecharse de un fallo para obtener las pulsaciones del teclado y otros datos sensibles que vayan por la memoria de los servidores que usen un procesador Xeon de Intel, incluso si está en un entorno virtual. Cada servidor ejecuta multitud de instancias individuales para cada usuario mediante virtualización, y un atacante puede acceder a los datos de otras personas que estén usando el mismo servidor; incluso aunque se estén escribiendo los datos en una sesión segura SSH.

Por parte de Intel, se ha visto obligada a recomendar a los usuarios que desactiven el DDIO y el RDMA, lo cual perjudica gravemente al rendimiento del sistema.

Esto demuestra lo inseguros que estamos hoy en día, porque… ¿Quién no usa un sistema operativo Android o IOS? O ¿Quién no usa Google Chrome? o... ¿Quién no usa un móvil con tarjeta SIM o un dispositivo IOT con tarjeta SIM? O… ¿Qué empresa no tiene mínimo un servidor con un Intel Xeon? Esto demuestra lo expuestos que estamos hoy en día, algo muy pero que muy preocupante.