Vulnerabilidad “BootHole”

BCSC_ALERTA_Vulnerabilidad_BootHole

TLP:WHITE

www.basquecybersecurity.eus

Julio 2020

TABLA DE CONTENIDO

Cláusula informativa

El presente documento se proporciona con el objeto de divulgar las alertas que el BCSC considera necesarias en favor de la seguridad de las organizaciones y de la ciudadanía interesada. En ningún caso el BCSC puede ser considerado responsable de posibles daños que, de forma directa o indirecta, de manera fortuita o extraordinaria pueda ocasionar el uso de la información revelada, así como de las tecnologías a las que se haga referencia tanto de la web de BCSC como de información externa a la que se acceda mediante enlaces a páginas webs externas, a redes sociales, a productos de software o a cualquier otra información que pueda aparecer en la alerta o en la web de BCSC. En todo caso, los contenidos de la alerta y las contestaciones que pudieran darse a través de los diferentes correos electrónicos son opiniones y recomendaciones acorde a los términos aquí recogidos no pudiendo derivarse efecto jurídico vinculante derivado de la información comunicada.

Cláusula de prohibición de venta

Queda terminantemente prohibida la venta u obtención de cualquier beneficio económico, sin perjuicio de la posibilidad de copia, distribución, difusión o divulgación del presente documento.

SOBRE EL BCSC

El Centro Vasco de Ciberseguridad (Basque Cybersecurity Centre, BCSC) es la entidad designada por el Gobierno Vasco para elevar el nivel de madurez de la ciberseguridad en Euskadi.

Es una iniciativa transversal que se enmarca en la Agencia Vasca de Desarrollo Empresarial (SPRI), sociedad dependiente del Departamento de Desarrollo Económico e Infraestructuras del Gobierno Vasco. Así mismo, involucra a otros tres Departamentos del Gobierno Vasco: el de Seguridad, el de Gobernanza Pública y Autogobierno, y el de Educación, y a cuatro agentes de la Red Vasca de Ciencia, Tecnología e Innovación: Tecnalia, Vicomtech, Ikerlan y BCAM.

El BCSC es la entidad de referencia para el desarrollo de la ciberseguridad y de la confianza digital de ciudadanos, empresas e instituciones públicas en Euskadi, especialmente para los sectores estratégicos de la economía de la región.

La misión del BCSC es por tanto promover y desarrollar la ciberseguridad en la sociedad vasca, dinamizar la actividad empresarial de Euskadi y posibilitar la creación de un sector profesional que sea referente. En este contexto se impulsa la ejecución de proyectos de colaboración entre actores complementarios en los ámbitos de innovación tecnológica, investigación y transferencia tecnológica a la industria de fabricación avanzada y otros sectores.

Así mismo, ofrece diferentes servicios en su rol como Equipo de Repuesta a Incidentes (en adelante CERT, por sus siglas en inglés “Computer Emergency Response Team”) y trabaja en el ámbito de la Comunidad Autónoma del País Vasco para aumentar la capacidad de detección y alerta temprana de nuevas amenazas, la respuesta y análisis de incidentes de seguridad de la información, y el diseño de medidas preventivas para atender a las necesidades de la sociedad vasca. Con el fin de alcanzar estos objetivos forma parte de diferentes iniciativas orientadas a la gestión de incidentes de ciberseguridad:

RESUMEN EJECUTIVO

Un equipo de investigadores de ciberseguridad ha revelado detalles de una nueva **vulnerabilidad de alto riesgo** que afecta a miles de millones de dispositivos en todo el mundo, incluidos servidores, equipos portátiles y de escritorio y sistemas IoT que ejecutan casi cualquier distribución de **Linux** o sistema **Windows**. Apodada "***BootHole***" e identificada con el **CVE-2020-10713**, la vulnerabilidad reside en el **gestor de arranque GRUB2**, que, si se explota, podría permitir a los atacantes eludir la función de arranque seguro y obtener acceso persistente y sigiloso de alto privilegio a los sistemas de destino. El problema también se extiende a cualquier dispositivo **Windows** que use el arranque seguro con la "*Third Party UEFI Certificate Authority*" de Microsoft.

La solución a esta vulnerabilidad no parece cercana a día de hoy ya que instalar parches con el gestor de arranque GRUB2 actualizado no resolvería el problema, puesto que los atacantes aún podrían reemplazar el gestor de arranque existente del dispositivo con la versión vulnerable. Por su parte, **Microsoft** publicó un aviso el 29 de julio reconociendo el problema e informó que "*está trabajando para completar la validación y las pruebas de compatibilidad de una actualización de Windows requerida que aborde esta vulnerabilidad*". También ha recomendado a los usuarios aplicar los parches de seguridad tan pronto como se implementen en las próximas semanas.

Además de Windows, muchas distribuciones populares de Linux y diferentes fabricantes también han publicado avisos relacionados notificando la vulnerabilidad, las posibles mitigaciones y la línea de tiempo para los próximos parches de seguridad:

- Red Hat (Fedora y RHEL)
- Canonical (Ubuntu)
- SuSE (SLES y OpenSUSE)
- Debian
- VMware
- HP

ANÁLISIS TÉCNICO

La vulnerabilidad "***BootHole***", referenciada con el identificador **CVE-2020-10713**, reside en el **gestor de arranque GRUB2**, utilizado por la mayoría de los sistemas **Linux** y afecta a los sistemas que utilizan el arranque seguro, incluso si no están utilizando GRUB2. El Arranque seguro es una característica de seguridad de UEFI (*Unified Extensible Firmware Interface*) que utiliza un cargador de arranque para cargar componentes críticos, periféricos y el sistema operativo, al tiempo que garantiza que solo se ejecute un código firmado criptográficamente durante el proceso de arranque.

Casi todas las versiones firmadas de GRUB2 son vulnerables, lo que significa que prácticamente todas las distribuciones de **Linux** se ven afectadas. Además, GRUB2 es compatible con otros sistemas operativos, núcleos e hipervisores como **Xen**. El problema también se extiende a cualquier dispositivo **Windows** que use el arranque seguro con la "*Third Party UEFI Certificate Authority*" de Microsoft.

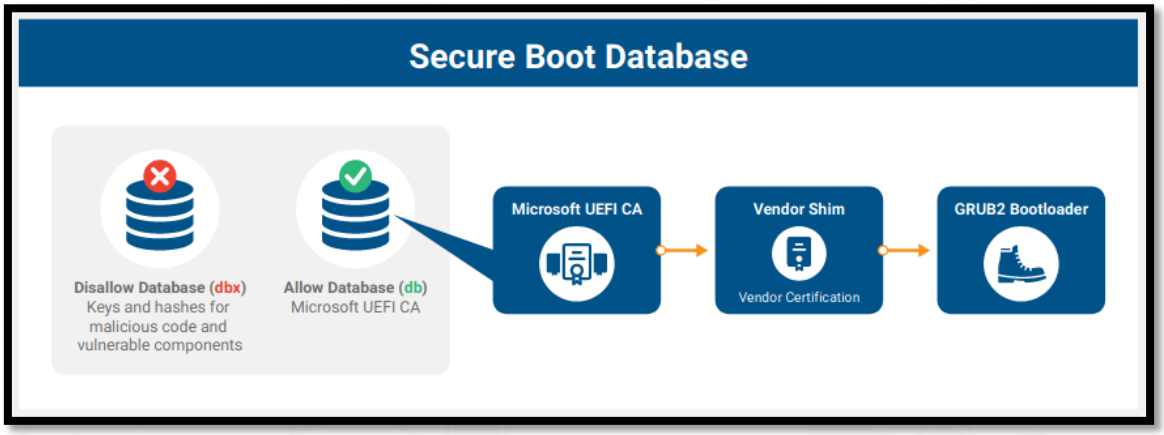

Ilustración 1. Ddetalle sobre el rol de la UEFI CA de Microsoft en el proceso de arranque

Por lo tanto, la mayoría de los equipos portátiles y de escritorio, servidores y estaciones de trabajo se ven afectados, así como dispositivos de red y otros equipos de propósito especial utilizados en entornos industriales, de salud y financieros. Este fallo hace que los dispositivos vulnerables sean susceptibles a posibles ataques mediante **cargadores de arranque UEFI malintencionados**.

"***BootHole***" es una vulnerabilidad de **desbordamiento de búfer** y se debe a la forma en la que se analiza el contenido del archivo de configuración **"grub.cfg"**, que generalmente no está firmado como otros archivos y ejecutables y se encuentra ubicado externamente, en la partición del sistema EFI. Un atacante podría modificar el archivo de configuración **"grub.cfg"** permitiéndole la ejecución de código dentro del entorno de ejecución UEFI, que podría usarse para ejecutar malware, alterar el proceso de arranque, parchear directamente el núcleo del sistema operativo o cualquier otra acción malintencionada, antes de que se inicie el sistema operativo, lo que dificulta la detección de la presencia de malware y su eliminación.

En sistemas **Windows**, los atacantes podrían proceder a reemplazar los cargadores de arranque predeterminados instalados por una versión vulnerable de GRUB2 para instalar un ***rootkit***. No obstante, Microsoft recalca que es necesario tener **privilegios administrativos o acceso físico** en un sistema donde el Arranque seguro está configurado para confiar en la "*Third Party UEFI Certificate Authority*" de Microsoft.

Ilustración 2. Recreación de ataque mediante la vulnerabilidad Boot Hole

MITIGACIÓN / SOLUCIÓN

Tal y como se ha mencionado anteriormente, la solución a esta vulnerabilidad no parece cercana a día de hoy ya que instalar parches con el gestor de arranque GRUB2 actualizado no resolvería el problema, puesto que los atacantes aún podrían reemplazar el gestor de arranque existente del dispositivo con la versión vulnerable.

Según los investigadores, una posible solución pasa por requerir que se firmen y se implementen **nuevos gestores de arranque**, a la vez que los gestores de arranque vulnerables son **revocados** para evitar que los atacantes utilicen versiones más antiguas y vulnerables. Por lo tanto, los proveedores afectados necesitarían primero lanzar las nuevas versiones de sus cargadores de arranque para ser firmadas por la UEFI CA de terceros de Microsoft. Además, la **lista de revocación UEFI (dbx)** también debería actualizarse en el firmware de cada sistema afectado para evitar la ejecución código vulnerable durante el arranque.

Por su parte, **Microsoft** ha publicado una serie de medidas de mitigación mientras trabaja en la publicación de un parche oficial que, según indican, estará disponible "*en las próximas semanas*". Es importante mencionar que estas mitigaciones no son compatibles con todo el software en todos los dispositivos, por lo que se recomienda verificar la compatibilidad antes de adoptar cualquier medida:

- **Reconfigurar el arranque seguro**: Microsoft Surface proporciona la capacidad de configurar el arranque seguro con o sin confianza en la UEFI CA de terceros. Los clientes de Surface que no requieren la UEFI CA de terceros pueden configurar el Arranque seguro como "Microsoft only" como una solución a este problema. Para más información, se recomienda consultar la siguiente guía: Manage Surface UEFI settings.

  ADVERTENCIA La modificación de la configuración de arranque seguro de UEFI puede desencadenar la recuperación de BitLocker y provocar fallos en otro software de seguridad. Se debe suspender BitLocker y tener la clave de recuperación de BitLocker disponible en caso de aplicar esta medida de mitigación.

- **Instalar manualmente la actualización DBX no probada**: En conjunto con la comunidad Linux, Microsoft lanzó una actualización no probada para abordar esta vulnerabilidad. Esta actualización opcional de DBX ha recibido pruebas limitadas y está destinada a profesionales. La actualización está alojada en el **Foro UEFI** en el siguiente enlace: https://uefi.org/revocationlistfile.

  ADVERTENCIA La instalación de este parche en sistemas incompatibles podría provocar un error de tiempo de ejecución, un bloqueo del sistema o incluso un fallo irrecuperable de arranque. Se recomienda consultar al fabricante correspondiente para determinar si su equipo es compatible.

REFERENCIAS ADICIONALES

- Eclypsium - There's a Hole in the Boot
- ADV200011 | Microsoft Guidance for Addressing Security Feature Bypass in GRUB
- Microsoft guidance for applying Secure Boot DBX update
- **UEFI Forum**: https://uefi.org/revocationlistfile
- **Canonical**: https://ubuntu.com/security/notices/USN-4432-1
- **Debian**: https://www.debian.org/security/2020-GRUB-UEFI-SecureBoot
- **HPE**: www.hpe.com/info/security-alerts
- **Red Hat**: https://access.redhat.com/security/vulnerabilities/grub2bootloader
- **SUSE**: https://www.suse.com/c/suse-addresses-grub2-secure-boot-issue/
- **VMware**: https://kb.vmware.com/s/article/80181

Reportar incidente

Si has detectado algún incidente de ciberseguridad, avísanos para que tomemos las medidas oportunas para evitar su propagación.

900 104 891

incidencias@bcsc.eus

Catálogo de ciberseguridad

¿Necesitas ayuda con tu ciberseguridad o la de tu empresa?