Un equipo de investigadores de seguridad cibernética reveló los detalles de una nueva vulnerabilidad de alto riesgo que afecta a miles de millones de dispositivos en todo el mundo, incluyendo servidores y estaciones de trabajo, computadoras portátiles, computadoras de escritorio y sistemas IoT que ejecutan casi cualquier distribución de Linux o sistema Windows.

Nombrada como BootHole y rastreado como CVE-2020-10713, la vulnerabilidad reportada reside en el gestor de arranque GRUB2, que de ser explotada, podría permitir a los hackers eludir la función de arranque seguro y obtener acceso persistente y sigiloso de alto privilegio a los sistemas de destino.

El arranque seguro es una característica de la interfaz de firmware extensible unificada (UEFI), que utiliza un cargador de arranque para cargar componentes críticos, periféricos y el sistema operativo al tiempo que garantiza que solo se ejecute el código firmado criptográficamente durante el proceso de arranque.

> *«Uno de los objetivos de diseño explícitos de Secure Boot es evitar que el código no autorizado, incluso con privilegios de administrador, obtenga privilegios adicionales y persistencia previa al SO deshabilitando Secure Boot o modificando la cadena de arranque»*, dice el informe de los investigadores.

Vulnerabilidad del cargador de arranque GRUB2

Descubierto por investigadores de Eclypsium, BootHole es una vulnerabilidad de desbordamiento de búfer que afecta a todas las versiones de GRUB2 y existe en la forma en que analiza el contenido del archivo de configuración, que generalmente no está firmado como otros archivos y ejecutables, lo que brinda a los atacantes la oportunidad de romper la raíz de hardware del mecanismo de confianza.

Para tener en cuenta, el archivo grub.cfg se encuentra en la partición del sistema EFI, y por lo

tanto, para modificar el archivo, un atacante necesita un punto de apoyo inicial en el sistema de destino con privilegios de administrador que eventualmente le proporcionarán al atacante una escalada adicional de privilegio y persistencia en el dispositivo.

Aunque GRUB2 es el gestor de arranque estándar utilizado por la mayoría de los sistemas Linux, también es compatible con otros sistemas operativos, núcleos e hipervisores como XEN.

> *«El desbordamiento del búfer permite al atacante obtener una ejecución de código arbitrario 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 ejecutar cualquier cantidad de acciones maliciosas»,* según los investigadores.

Para explotar la vulnerabilidad BootHole en sistemas Winows, los atacantes pueden reemplazar los cargadores de arranque predeterminados en sistemas Windows con una versión vulnerable de GRUB2 para instalar rootkit.

> *«El problema también se extiende a cualquier dispositivo de Windows que utilice el arranque seguro con la Autoridad de Certificación UEFI de terceros de Microsoft»*, dice el informe.

Según el informe detallado, la vulnerabilidad puede tener graves consecuencias, y eso se debe principalmente a que el ataque permite a los hackers ejecutar código malicioso aún antes de que se inicie el sistema operativo, lo que dificulta que el software de seguridad detecte la presencia de malware o eliminarlo.

Además, los investigadores agregaron que *«el entorno de ejecución de UEFI no tiene la asignación aleatoria del diseño del espacio de direcciones (ASLR) o la prevención de*

ejecución de datos (DEP/NX) u otras tecnologías de mitigación de exploits que normalmente se encuentran en los sistemas operativos modernos, por lo que crear exploits para este tipo de vulnerabilidad es significativamente más difícil».

Los expertos de Eclypsium ya se pusieron en contacto con entidades relacionadas de la industria, incluyendo los proveedores de sistemas operativos y fabricantes de computadoras, para ayudarlos a solucionar el problema.

El simple hecho de instalar parches con el gestor de arranque GRUB2 actualizado, no resolverá el problema, debido a que los atacantes aún pueden reemplazar el gestor de arranque existente del dispositivo con la versión vulnerable.

Segpun Eclypsium, la *«mitigación requerirá que se firmen y se implementen nuevos gestores de arranque, y los gestores de arranque vulnerables deberían ser revocados para evitar que los adversarios utilicen versiones más antiguas y vulnerables en un ataque».*

Por lo tanto, los proveedores afectados necesitarían primero lanzar las nuevas versiones de sus calzas de cargador de arranque para ser firmados por la UEFI CA de terceros de Microsoft.

Finalmente, la lista de revocación UEFI (dbx) también debe actualizarse en el firmware de cada sistema afectado para evitar ejecutar el código vulnerable durante el arranque.

Probablemente, el proceso de mitigación de múltiples etapas lleve años, debido al tiempo que requieren las organizaciones para completar los parches.

> *«Sin embargo, la implementación completa de este proceso de revocación probablemente será muy lenta. Las actualizaciones relacionadas con UEFI han tenido un historial de inutilización de dispositivos, y los proveedores deberán ser muy cautelosos. Si la lista de revocación (dbx) se actualiza antes de un Linux dado,*

> *y el gestor y la cuña se actualizan, luego el sistema operativo no se cargará»,* dicen los investigadores.

Microsoft emitió un aviso en el que reconoce el problema y dijo que se *«está trabajando para completar la validación y las pruebas de compatibilidad de una actualización de Windows requerida que aborde esta vulnerabilidad»*.

También recomendó a los usuarios aplicar parches de seguridad tan pronto como se implementen en las siguientes semanas.

Además de Microsoft, muchas distribuciones populares de Linux también publicaron avisos relacionados que explican la falla, las posibles mitigaciones y la línea de tiempo en los próximos parches de seguridad, como Red Hat, Canonical, SuSE, Debian, VMware y HP.