Algunos distribuidores de Linux lanzaron parches para BootHole, el problema de seguridad recientemente revelado que involucra GRUB2 y Secure Boot, que puede utilizarse para atacar sistemas Linux. Pero algunos de los parches causaron otros problemas.

Desafortunadamente, los parches para algunas distribuciones de Linux, incluyendo Red Hat, resultaron peor que el problema de seguridad en sí, pues algunos usuarios se encontraron con el problema de que los sistemas *«reparados»* ya no arrancaban.

Peter Allor, director del Equipo de Respuesta a Incidentes de Seguridad de Productos de Red Hat dijo:

> *«Red Hat ha sido informado de un posible problema con la solución para CVE-2020-10713, también conocido como BootHole, por el cual algunos sistemas Red Hat Enterprise Linux 7 y Red Hat Enterprise Linux 8 puede no reiniciarse con éxito después de aplicar la corrección, lo que requiere intervención manual para arreglar. Actualmente estamos investigando este problema y proporcionaremos más información a medida que esté disponible».*

La solución tardó varios días y no unas pocas horas para poder obtener éxito. Ahora, está lista la solución para su implementación en Red Hat Enterprise Linux (RHEL) 7.8 y 8.2. Aunque la solución no se ha confirmado para RHEL 7.9 y 2.1 Exdended Update Support (EUS), también debería funcionar en ellos.

La reparación consiste en paquetes de cuñas actualizados. Una cuña en este contexto es un certificado de arranque seguro UEFI (Unified Extensible Firmware Interface). Está firmado por el distribuidor de Linux, que está implícitamente confiado al estar integrado en el cargador de suplementos firmado de Microsoft.

El arranque seguro UEFI de Microsoft se usa porque casi todas las computadoras vienen precargadas con las claves de arranque seguro de Microsoft.

Estos paquetes de shim actualizados están disponibles ahora. Se pueden usar con los paquetes GRUB2, fwupd y fwupdate publicados anteriormente.

Para realizar una corrección, es necesario reiniciar el sistema utilizando el DVD RHEL en modo de solución de problemas. Una vez arrancado, ingresar al contenedor chroot y reemplazar el paquete de cuñas defectuoso con la versión reparada.

Con el sistema operativo clon RHEL CentOS, el proceso es muy similar, sin embargo, es recomendable leer el informe de errores de reparación de CentOS BootHole. En lugar de volver a una cuña de arranque antigua, como se describe al comienzo del informe, se actualizará a shimx64-15-15.el8_2.x86_64.rpm (EL8), shim-x64-15-8.el7_8 respectivamente, o más nuevo, x.86_64.rpm.

Según empleados de Red Hat, el problema del sistema no arrancable nunca afectó a Fedora, la distribución de Linux de la comunidad de Red Hat. Los programadores de Fedora están trabajando actualmente en la entrega de una solución amplia para BootHole.

> *«Dicho esto, dada la superficie de ataque muy estrecha de BootHole (que ya requiere acceso, etc.) se considera un problema grave pero no demasiado crítico».*

Canonical, la compañía matriz de Ubuntu, informó que se ha visto muy pocas instancias de sistemas que no arrancan con su parche BootHole. Pero para esos pocos casos, sugiere degradar grub a grub2-signed desde otra sesión de Ubuntu.

Con una máquina local se puede hacer con un DVD Ubuntu o una Live USB. En la nube se puede hacer desde una instancia separada en la misma zona de disponibilidad de la nube. De cualquier forma, utiliza los mismos pasos finales. Es decir, montar el volumen/dispositivo raíz del sistema afectado en la instancia de nube en vivo/separada, realizar un corte en él y usar apt para degradar grub2/grub2-signed.

En el caso de Debian Linux, la corrección de BootHole se integra en la última versión de

Debian 10 «Buster», Debian 10.5.