DINI	**ALERTA INTEGRADA DE SEGURIDAD DIGITAL N° 101**	**Fecha: 29-04-2023**
		Página 7 de 11

Componente que reporta	**DIRECCIÓN NACIONAL DE INTELIGENCIA**		
Nombre de la alerta	Múltiples vulnerabilidades en el kernel de Linux de RedHat		
Tipo de ataque	Explotación de vulnerabilidades conocidas	Abreviatura	EVC
Medios de propagación	Red, Internet		
Código de familia	H	Código de subfamilia	H01
Clasificación temática familia	Intento de intrusión		

Descripción

1. **Resumen:**

Red HAT ha reportado una vulnerabilidad de severidad **ALTA** de tipo escritura fuera de los límites y gestión de propiedad inadecuada en el kernel de Linux de RedHat. La explotación exitosa de estas vulnerabilidades podría permitir a un atacante remoto generar una condición de denegación de servicio (DoS) y la escalada de privilegios.

2. **Detalles:**

- La vulnerabilidad de severidad **alta** registrada como CVE-2022-43750 en el kernel de Linux, podría permitir la corrupción de memoria en el controlador **usbmon**. La vulnerabilidad existe debido a una falla de escritura de memoria fuera de los límites en el componente USB Monitor del kernel de Linux en la forma en que un usuario con acceso a **/dev/usbmon** puede activarlo mediante una escritura incorrecta en la memoria de **usbmon**. Esta falla permite que un usuario local bloquee o aumente potencialmente sus privilegios en el sistema.

- La vulnerabilidad de severidad **alta** registrada como CVE-2023-0386 en el kernel de Linux, podría permitir a un usuario con bajos privilegios elevar privilegios en el sistema de archivos FUSE. La vulnerabilidad existe debido a una falla en el kernel de Linux, donde se encontró acceso no autorizado a la ejecución del archivo **setuid** con capacidades en el subsistema **OverlayFS** del kernel de Linux en la forma en que un usuario copia un archivo capaz de un montaje **nosuid** a otro montaje. Este error de asignación de **uid** permite que un usuario local aumente sus privilegios en el sistema.

3. **Productos afectados:**

- Red Hat CodeReady Linux Builder para ARM 64 - Soporte de actualización extendida 9.0 aarch64;
- Red Hat CodeReady Linux Builder para IBM z Systems - Soporte de actualización extendido 9.0 s390x;
- Red Hat CodeReady Linux Builder for Power, little endian - Soporte de actualización extendido 9.0 ppc64le;
- Red Hat CodeReady Linux Builder para x86_64 - Soporte de actualización extendido 9.0 x86_64;
- Escritorio Red Hat Enterprise Linux 7 x86_64;
- Servidor Red Hat Enterprise Linux 7 x86_64;
- Red Hat Enterprise Linux Server para ARM 64 - 4 años de actualizaciones 9.0 aarch64;
- Red Hat Enterprise Linux Server para IBM z Systems - 4 años de actualizaciones 9.0 s390x;
- Red Hat Enterprise Linux Server para Power LE: servicios de actualización para soluciones SAP 9.0 ppc64le;
- Estación de trabajo Red Hat Enterprise Linux 7 x86_64;
- Red Hat Enterprise Linux para ARM 64 - Soporte de actualización extendido 9.0 aarch64;
- Red Hat Enterprise Linux para IBM z Systems - Soporte de actualización extendido 9.0 s390x;
- Red Hat Enterprise Linux para IBM z Systems 7 s390x;
- Red Hat Enterprise Linux para Power, big endian 7 ppc64;
- Red Hat Enterprise Linux para Power, little endian - Soporte de actualización extendido 9.0 ppc64le;
- Red Hat Enterprise Linux para Power, little endian 7 ppc64le;
- Red Hat Enterprise Linux para tiempo real 7 x86_64;
- Red Hat Enterprise Linux en tiempo real para NFV 7 x86_64;
- Red Hat Enterprise Linux para informática científica 7 x86_64;
- Red Hat Enterprise Linux para x86_64 - Soporte de actualización extendida 9.0 x86_64;
- Red Hat Enterprise Linux para x86_64 - Servicios de actualización para soluciones SAP 9.0 x86_64.

4. Solución:

- Red Hat recomienda actualizar los productos afectados con la última versión de software disponible que abordan estas vulnerabilidades.

Fuentes de información	▪ hxxps://access.redhat.com/errata/RHSA-2023:1970 ▪ hxxps://access.redhat.com/errata/RHSA-2023:1988 ▪ hxxps://access.redhat.com/errata/RHSA-2023:1987