BOLETÍN DE ALERTA

Boletín Nro.: 2023-20
Fecha de publicación: 12/05/2023
Fecha de actualización: 18/05/2023
Tema: Vulnerabilidad crítica en componente *Netfilter (configurable con iptables)* del *kernel* de Linux – Actualización.

El software afectado es:

- *Kernel* Linux, versión 6.3.1 y anteriores.

Descripción:

Se ha reportado un nuevo aviso de seguridad sobre una vulnerabilidad de gestión de memoria que afecta al componente *kernel* de Linux llamado Netfilter, que permitiría a un atacante local autenticado ejecutar y obtener escalamiento de privilegios en el sistema afectado.

Netfilter es un *framework* del *kernel* Linux que provee servicios de filtrado de paquetes y manipulación de red, trabaja conjuntamente con la herramienta *iptables*. La cual es una herramienta de línea de comandos que utiliza el *framework* Netfilter para configurar reglas de filtrado de paquetes en el sistema.

La vulnerabilidad es identificada como CVE-2023-32233, de severidad "Crítica" y sin puntuación asignada aún. Se encontró una falla *use-after-free* (*UAF*) en la funcionalidad de Netfilter *nf_tables* que permite actualizar su configuración con peticiones por lotes que agrupan múltiples operaciones básicas en transacciones atómicas. Esto permitiría a un atacante local autenticado a través del envío de una solicitud por lotes especialmente diseñada, realizar operaciones arbitrarias de lectura y escritura en la memoria y obtener privilegios elevados como usuario *root* en el sistema afectado. Actualmente para esta vulnerabilidad existe prueba de concepto (*PoC*) publicada.

Impacto:

La explotación exitosa de esta vulnerabilidad podría permitir a un atacante local realizar operaciones arbitrarias de lectura y escritura en la memoria y obtener privilegios elevados como usuario *root* en el sistema afectado.

Solución:

Recomendamos instalar las actualizaciones correspondientes para la distribución Debian a través del siguiente enlace:

- Bullseye (security) 5.10.179-1

Mitigación:

Actualmente los desarrolladores del código del *kernel* de Linux están trabajando en *un patch 6.4-rc1* como solución temporal para la vulnerabilidad:

- https://www.debugpoint.com/linux-kernel-6-4-rc1/
- https://git.kernel.org/pub/scm/linux/kernel/git/torvalds/linux.git/patch/?id=c1592a89942e9678f7d9c8030efa777c0d57edab
- https://security-tracker.debian.org/tracker/CVE-2023-32233
- https://www.linuxcompatible.org/story/linux-kernel-64rc1-released/

Si desea puede acceder al *patch 6.4-rc1* pero recordamos que aún está en fase de testeo, no se recomienda para ambientes de producción:

- https://www.kernel.org/

Adicionalmente, como esta vulnerabilidad aún se encuentra en curso de investigación recomendamos permanecer informados con relación a las actualizaciones oficiales que serán lanzadas por parte del equipo de Linux.

Información adicional:

- https://www.cert.gov.py/noticias/vulnerabilidad-de-escalamiento-de-privilegios-en-el-kernel-de-linux-4/
- https://securityonline.info/cve-2023-32233-linux-kernel-privilege-escalation-a-critical-security-vulnerability-uncovered/
- https://www.debugpoint.com/linux-kernel-6-4-rc1/
- https://security-tracker.debian.org/tracker/CVE-2023-32233
- https://www.openwall.com/lists/oss-security/2023/05/08/4
- https://nvd.nist.gov/vuln/detail/CVE-2023-32233
- https://git.kernel.org/pub/scm/linux/kernel/git/torvalds/linux.git/patch/?id=c1592a89942e9678f7d9c8030efa777c0d57edab
- https://www.debian.org/security/2023/dsa-5402
- https://securityonline.info/poc-released-for-linux-kernel-privilege-escalation-cve-2023-32233-vulnerability/