La Agencia de Seguridad de Infraestructura y Ciberseguridad de Estados Unidos (CISA), agregó esta semana una vulnerabilidad de Linux denominada PwnKit a su Catálogo de Vulnerabilidades Explotadas Conocidas, citando evidencia de explotación activa.

La vulnerabilidad, rastreada como CVE-2021-4034 con puntuación CVSS de 7.8, salió a la luz en enero de 2022 y se refiere a un caso de escalada de privilegios locales en la utilidad pkexec de polkit, que permite a un usuario autorizado ejecutar comandos como otro usuario.

Polkit (anteriormente llamado PolicyKit) es un conjunto de herramientas para controlar los privilegios de todos el sistema en sistemas operativos similares a Unix, y proporciona un mecanismo para que los procesos sin privilegios se comuniquen con los procesos privilegiados.

La explotación exitosa de la vulnerabilidad podría inducir a pkexec a ejecutar código arbitrario, otorgando a un atacante sin privilegios los derechos administrativos en la máquina de destino y comprometiendo el host.

Aún no está claro cómo se está armando la vulnerabilidad en la naturaleza, ni existe información sobre la identidad del atacante de que puede estar explotándola.

También se incluye en el catálogo CVE-2021-30533, una vulnerabilidad de seguridad en los navegadores web basados en Chromium, que fue aprovechada por un atacante de publicidad maliciosa con nombre en código Yosex para entregar cargas útiles peligrosas el año pasado.

Además, la agencia agregó el día cero Mitel VoIP recientemente revelado (CVE-2022-29499), así como cinco vulnerabilidades de Apple iOS (CVE-2018-4344, CVE-2019-8605, CVE-2020-9907, CVE-2020-3837 y CVE-2021-30983) que recientemente se descubrió que habían sido objetos de abuso por parte del proveedor italiano de spyware RCS Lab.

Para mitigar cualquier riesgo potencial de exposición a ataques cibernéticos, se recomienda que las organizaciones den prioridad a la corrección oportuna de los problemas. Sin embargo, las agencias del poder ejecutivo civil federal deben corregir obligatoriamente la

vulnerabilidad antes del 18 de julio de 2022.