La Agencia de Seguridad de Infraestructura y Ciberseguridad de EE. UU. (CISA) ha incorporado una vulnerabilidad crítica que afecta a Jenkins en su catálogo de Vulnerabilidades Conocidas Explotadas (KEV), tras ser utilizada en ataques de ransomware.

La vulnerabilidad, identificada como CVE-2024-23897 (con una puntuación CVSS de 9.8), es una falla de recorrido de rutas que podría permitir la ejecución de código.

> *«La Interfaz de Línea de Comandos (CLI) de Jenkins contiene una vulnerabilidad de recorrido de rutas que otorga a los atacantes acceso limitado a ciertos archivos, lo que podría llevar a la ejecución de código»,* explicó CISA en un comunicado.

Este problema fue reportado por primera vez por investigadores de seguridad de Sonar en enero de 2024 y fue solucionado en las versiones 2.442 y LTS 2.426.3 de Jenkins al deshabilitar la función del analizador de comandos.

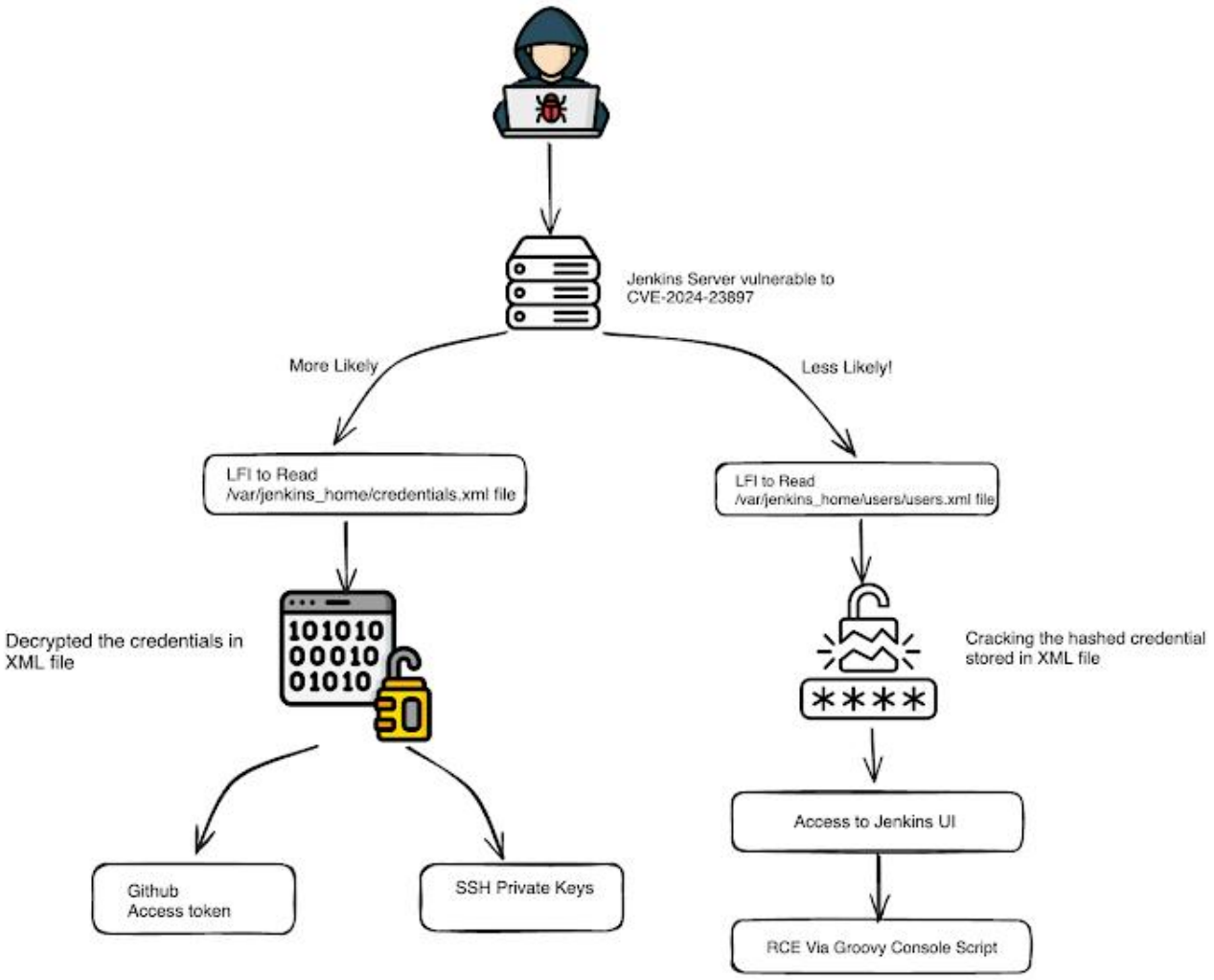
En marzo, Trend Micro reveló que descubrió varios ataques originados en los Países Bajos, Singapur y Alemania, y que detectó casos en los que se estaban intercambiando activamente exploits para la ejecución remota de código utilizando esta vulnerabilidad.

En semanas recientes, CloudSEK y Juniper Networks han informado sobre una serie de ciberataques que explotan la vulnerabilidad CVE-2024-23897 para infiltrarse en las compañías BORN Group y Brontoo Technology Solutions.

Estos ataques han sido atribuidos al actor de amenazas conocido como IntelBroker y al grupo de ransomware RansomExx.

> *«CVE-2024-23897 es una vulnerabilidad LFI no autenticada que permite a los atacantes leer archivos arbitrarios en el servidor Jenkins. Esta vulnerabilidad se origina debido a una validación incorrecta de entradas, lo que permite a los atacantes manipular ciertos parámetros y engañar al servidor para que acceda y*

> *muestre el contenido de archivos sensibles»,* indicó CloudSEK.



Debido a la explotación activa de esta vulnerabilidad, las agencias de la Rama Ejecutiva Civil Federal (FCEB) tienen hasta el 9 de septiembre de 2024 para aplicar las correcciones y proteger sus redes contra amenazas activas.