Se han revelado múltiples vulnerabilidades de inyección SQL en Gentoo Soko que podrían llevar a la ejecución remota de código (RCE) en sistemas vulnerables.

«A pesar del uso de una biblioteca de asignación objeto-relacional (ORM) y declaraciones preparadas, estas inyecciones SQL se produjeron», señaló Thomas Chauchefoin, investigador de SonarSource, añadiendo que podrían dar lugar a RCE en Soko debido a una *«configuración incorrecta de la base de datos».*

Estas dos vulnerabilidades, descubiertos en la función de búsqueda de Soko, han sido identificados colectivamente como CVE-2023-28424 (puntuación CVSS: 9.1). Se tomaron medidas para abordarlos en un plazo de 24 horas después de su divulgación responsable el 17 de marzo de 2023.

Soko es un módulo de software en Go que impulsa packages.gentoo.org, ofreciendo a los usuarios una forma sencilla de buscar diferentes paquetes de Portage disponibles para la distribución de Linux Gentoo.

Sin embargo, las limitaciones identificadas en el servicio significaban que podría haber existido la posibilidad de que un actor malintencionado pudiera insertar código especialmente creado, lo que resultaría en la exposición de información confidencial.

> *«Las infiltraciones SQL eran explotables y tenían la capacidad de revelar la versión del servidor PostgreSQL y ejecutar comandos arbitrarios en el sistema»,* mencionó SonarSource.

Este avance se produce meses después de que SonarSource descubriera una vulnerabilidad de script entre sitios (XSS) en un conjunto de herramientas empresariales de código abierto llamado Odoo, que podría ser aprovechada para suplantar a cualquier víctima en una instancia vulnerable de Odoo, así como para extraer información valiosa.

A principios de este año, también se divulgaron debilidades de seguridad en software de

código abierto como Pretalx y OpenEMR, que podrían allanar el camino para que atacantes remotos ejecuten código arbitrario.