Se han revelado cuatro fallos de seguridad no parcheados, incluidos tres críticos, en el servicio Git autoalojado y de código abierto Gogs. Estos fallos podrían permitir a un atacante autenticado comprometer instancias vulnerables, robar o borrar código fuente, e incluso insertar puertas traseras.

Las vulnerabilidades, según los investigadores de SonarSource Thomas Chauchefoin y Paul Gerste, son las siguientes:

- CVE-2024-39930 (puntuación CVSS: 9.9) – Inyección de argumentos en el servidor SSH integrado.
- CVE-2024-39931 (puntuación CVSS: 9.9) – Eliminación de archivos internos.
- CVE-2024-39932 (puntuación CVSS: 9.9) – Inyección de argumentos durante la vista previa de cambios.
- CVE-2024-39933 (puntuación CVSS: 7.7) – Inyección de argumentos al etiquetar nuevas versiones.

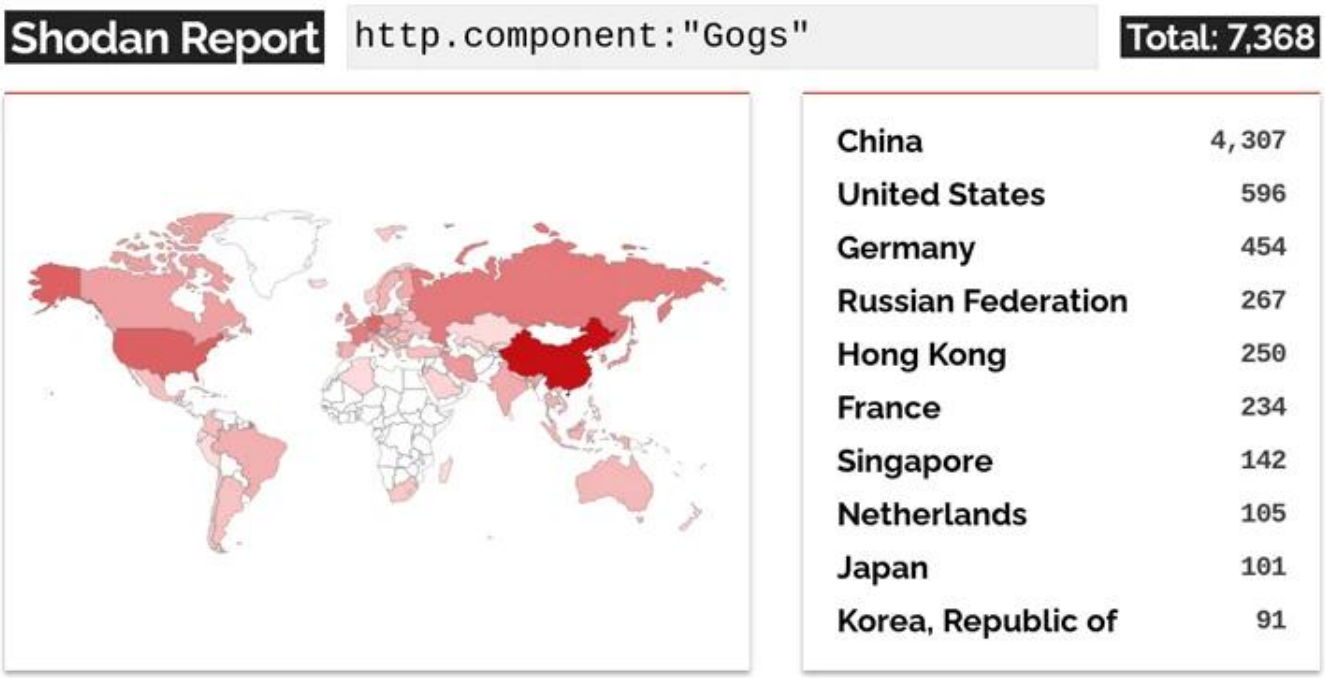
La explotación exitosa de las tres primeras vulnerabilidades podría permitir a un atacante ejecutar comandos arbitrarios en el servidor Gogs, mientras que la cuarta vulnerabilidad permite a los atacantes leer archivos arbitrarios como código fuente y secretos de configuración.

En otras palabras, al aprovechar estos problemas, un atacante podría leer el código fuente en la instancia, modificar cualquier código, eliminar todo el código, atacar hosts internos accesibles desde el servidor Gogs e impersonar a otros usuarios para obtener más privilegios.

Sin embargo, las cuatro vulnerabilidades requieren que el atacante esté autenticado. Además, desencadenar la CVE-2024-39930 requiere que el servidor SSH integrado esté habilitado, la versión del binario utilizada, y que el atacante posea una clave privada SSH válida.

> *«Si la instancia de Gogs tiene habilitado el registro, el atacante puede simplemente crear una cuenta y registrar su clave SSH. De lo contrario, tendrían que comprometer otra cuenta o robar la clave privada SSH de un usuario»*, explicaron los investigadores.

Las instancias de Gogs que se ejecutan en Windows no son vulnerables, al igual que la imagen de Docker. Sin embargo, las que se ejecutan en Debian y Ubuntu son susceptibles debido a que el binario env soporta la opción `--split-string`.



Según datos de Shodan, alrededor de 7,300 instancias de Gogs son accesibles públicamente en Internet, con casi el 60% ubicadas en China, seguidas por EE. UU., Alemania, Rusia y Hong Kong.

Actualmente, no está claro cuántos de estos servidores expuestos son vulnerables a los fallos

mencionados. SonarSource dijo que no tiene visibilidad sobre si estos problemas están siendo explotados activamente.

La firma suiza de ciberseguridad también señaló que los mantenedores del proyecto *«no implementaron correcciones y dejaron de comunicarse»* después de aceptar su informe inicial el 28 de abril de 2023.

En ausencia de una actualización, se recomienda a los usuarios desactivar el servidor SSH integrado, desactivar el registro de usuarios para prevenir la explotación masiva y considerar cambiarse a Gitea. SonarSource también ha lanzado un parche que los usuarios pueden aplicar, aunque señalaron que no ha sido probado exhaustivamente.

Esta revelación coincide con el descubrimiento de la empresa de seguridad en la nube Aqua de que información sensible, como tokens de acceso y contraseñas, una vez codificados, pueden permanecer expuestos de forma permanente incluso después de ser eliminados de los sistemas de gestión de código fuente basados en Git (SCM).

Llamados secretos fantasma, el problema surge porque no pueden ser descubiertos por los métodos de escaneo convencionales –la mayoría de los cuales buscan secretos usando el comando `git clone`– y porque ciertos secretos son accesibles solo a través de `git clone --mirror` o vistas en caché de las plataformas SCM, destacando los puntos ciegos que dichas herramientas de escaneo pueden pasar por alto.

> *«Los commits permanecen accesibles a través de 'vistas en caché' en el SCM. Esencialmente, el SCM guarda el contenido del commit para siempre»,* explicaron los investigadores de seguridad Yakir Kadkoda e Ilay Goldman.
>
> *«Esto significa que incluso si un commit que contiene un secreto es eliminado de ambas versiones clonadas y reflejadas de su repositorio, aún puede ser accesible si alguien conoce el hash del commit. Pueden recuperar el contenido del commit a través de la GUI de la plataforma SCM y acceder al secreto filtrado».*