**GitHub Dependabot**

Muchas aplicaciones o proyectos requieren de dependencias para su correcto funcionamiento, pero cuando estas dependencias no están actualizadas, podrían causar muchos problemas con la seguridad, adicional la actualización manual de estas dependencias y la comprobación de actualizaciones pueden ser estresantes.

**Dependencias**

En el campo del software una dependencia es una aplicación o una biblioteca requerida por otro programa para poder funcionar correctamente. Por ello se dice que dicho programa depende de tal aplicación o biblioteca.

**¿Qué es Dependabot?**

Dependabot ayuda a los usuarios de tu instancia de GitHub Enterprise Server a encontrar y corregir vulnerabilidades en sus dependencias.

Con Las alertas del dependabot, GitHub identifica dependencias vulnerables en repositorios y crea alertas en tu instancia de GitHub Enterprise Server, utilizando datos de la base de datos de asesoramiento de GitHub y el servicio de gráficos de dependencias.

Agregamos vulnerabilidades a la GitHub Advisory Database desde las siguientes fuentes:

* La Base Nacional de Datos de Vulnerabilidades.
* Una combinación de aprendizaje automático y revisión humana para detectar vulnerabilidades en confirmaciones públicas en GitHub
* Asesorías de seguridad que se reportan en GitHub
* La base de datos de Asesorías de seguridad de npm database

Después de habilitar Las alertas del dependabot para su empresa, los datos de vulnerabilidad se sincronizan desde la base de datos de asesoramiento de GitHub a su instancia una vez cada hora. Solo se sincronizan los avisos revisados ​​por GitHub. Para obtener más información sobre los datos de las asesorías, consulte la sección "Buscar vulnerabilidades de seguridad en la GitHub Advisory Database" dentro de la documentación de GitHub.com.

También puede optar por sincronizar manualmente los datos de vulnerabilidad en cualquier momento. Para obtener más información, consulte "Visualización de los datos de vulnerabilidad de su empresa".

**Habilitar Las alertas del dependabot**

[Habilitación de Dependabot para tu empresa - GitHub Docs](https://docs.github.com/es/enterprise-server@3.0/admin/configuration/configuring-github-connect/enabling-dependabot-for-your-enterprise)

Dependabot es una herramienta ya totalmente integrada con github, que podemos utilizar para automatizar el análisis y las actualizaciones de dependencias de nuestros proyectos desarrollados.

**GitHub Security Advisory**

Dependabot aprovecha la api de **GitHub Security Advisory** para automatizar el proceso y crear solicitudes de extracción para corregir vulnerabilidades a medida que se encuentran.

**GitHub Security Advisory**: Detrás de las características de seguridad de GitHub hay una base de datos cuidadosamente seleccionada de vulnerabilidades de seguridad agregadas de toda la web. Estos datos ahora están disponibles para todos los desarrolladores con la API de asesoramiento de seguridad.

Al poder acceder a la api de **Security Advisory,** Dependabot puede:

* automatizar el proceso de monitoreo.
* ayudar a verificar los avisos de seguridad en los archivos de dependencia.
* crea solicitudes de extracción (pull requests) para corregir las vulnerabilidades a medida que se encuentran.

Cabe mencionar que Dependabot no solo crea solicitudes de extracción para vulnerabilidades de seguridad de forma predeterminada, sino que creará solicitudes de extracción siempre que haya una actualización disponible.

Agregamos vulnerabilidades a la GitHub Advisory Database desde las siguientes fuentes:

* La Base Nacional de Datos de Vulnerabilidades
* Una combinación de aprendizaje automático y revisión humana para detectar vulnerabilidades en confirmaciones públicas en GitHub
* Asesorías de seguridad que se reportan en GitHub
* La base de datos de Asesorías de seguridad de npm database

**Las alertas del dependabot**

GitHub puede crear Las alertas del dependabot cuando detecta dependencias vulnerables en tu repositorio. La alerta se muestra en la ficha Seguridad del repositorio. La alerta incluye un vínculo al archivo afectado en el proyecto e información sobre una versión fija. GitHub también notifica a los mantenedores del repositorio, de acuerdo con sus preferencias de notificación. Para obtener más información, consulte "Acerca de las alertas para dependencias vulnerables".

**Actualizaciones de seguridad del dependabot**

Cuando GitHub genera una alerta de Dependabot para una dependencia vulnerable en su repositorio, Dependabot puede intentar solucionarlo automáticamente por usted. Las actualizaciones de seguridad del dependabot son solicitudes de extracción generadas automáticamente que actualizan una dependencia vulnerable a una versión fija. Para obtener más información, consulte "Acerca de Actualizaciones de seguridad del dependabot".

**Gráfico de dependencias**

El gráfico de dependencias es un resumen de los archivos de manifiesto y bloqueo almacenados en un repositorio. Le muestra los ecosistemas y paquetes de los que depende su base de código (sus dependencias) y los repositorios y paquetes que dependen de su proyecto (sus dependientes). La información del gráfico de dependencias es utilizada por dependency review y Dependabot. Para obtener más información, consulte "Acerca del gráfico de dependencias".

**Acerca del archivo dependabot.yml**

El archivo de configuración de Dependabot, dependabot.yml, utiliza la sintaxis YAML. Si es nuevo en YAML y desea obtener más información, consulte "Aprender YAML en cinco minutos".

Debe almacenar este archivo en el directorio de su repositorio. Al agregar o actualizar el archivo dependabot.yml, esto desencadena una comprobación inmediata de las actualizaciones de versión.

Cualquier opción que también afecte a las actualizaciones de seguridad se usará la próxima vez que una alerta de seguridad active una solicitud de extracción para una actualización de seguridad.

El archivo dependabot.yml tiene dos claves de nivel superior obligatorias: , y . Opcionalmente, puede incluir una clave de nivel superior. El archivo debe comenzar con .version updates registries version: 2

[¡Adiós Dependabot Preview, hola Dependabot! | El blog de GitHub](https://github.blog/2021-04-29-goodbye-dependabot-preview-hello-dependabot/)

[Mantenga todos sus paquetes actualizados con Dependabot | El blog de GitHub](https://github.blog/2020-06-01-keep-all-your-packages-up-to-date-with-dependabot/)