05/07/22

Vulnerabilidad de alta gravedad corregida en Django

El proyecto Django, un framework web de código abierto basado en Python, ha reparado una vulnerabilidad de alta gravedad en sus últimas versiones.

Identificada como **CVE-2022-34265**, la **vulnerabilidad** potencial de **inyección SQL** existe en la rama principal de Django y en las versiones 4.1 (actualmente en versión beta), 4.0 y 3.2. Los nuevos lanzamientos y parches emitidos este lunes 4 de julio eliminan la vulnerabilidad.

Decenas de miles de empresas eligen Django como framework base para sus sitios web. Esto hace todavía más **urgente la necesidad de actualizar o parchear** las instancias de Django contra errores como estos.

El equipo de Django ha lanzado las versiones Django 4.0.6 y Django 3.2.14 que abordan una vulnerabilidad de inyección SQL de alta gravedad e insta a los desarrolladores a actualizar o parchear sus instancias de Django lo antes posible.

La vulnerabilidad puede permitir que un actor de amenazas ataque las aplicaciones web de Django a través de argumentos proporcionados a las funciones **Trunc()** y **Extract()**.

«Las funciones de base de datos Trunc() y Extract() estaban sujetas a la inyección de SQL si se usaban datos que no eran de confianza como un valor de **tipo/lookup_name**«.

«Las aplicaciones que restringen el lookup name y la elección de tipo a una lista segura conocida no se ven afectadas».

En otras palabras, su aplicación no es vulnerable si está realizando algún tipo de desinfección de entrada o escapando antes de pasar estos argumentos a las funciones Trunc y Extract.

Se le atribuye al investigador Takuto Yoshikai de Aeye Security Lab el informe responsable de la vulnerabilidad.

Para aquellos que no pueden actualizar a las versiones fijas de Django 4.0.6 o 3.2.14, el equipo ha puesto a disposición parches que se pueden aplicar a las versiones afectadas existentes.

Se han aplicado parches para resolver el problema en la rama principal de Django y en las ramas de las versiones 4.1, 4.0 y 3.2. Los parches se pueden obtener de los siguientes conjuntos de cambios del proyecto:

Rama principal
Rama de versión 4.1
Rama de versión 4.0
Rama de versión 3.2

«Esta versión de seguridad mitiga el problema, pero hemos identificado mejoras en los métodos de la API de la base de datos relacionados con la extracción y el truncado de fechas que sería beneficioso agregar a Django 4.1 antes de su versión final», afirma además el equipo de Django.

«Esto afectará a los backends de bases de datos de terceros que utilizan la versión candidata 1 o posterior de Django 4.1, hasta que puedan actualizar los cambios de la API. Nos disculpamos por las molestias».

La política de seguridad de Django establece que cualquier posible problema de seguridad se informe de forma privada por correo electrónico a **security@djangoproject.com**, en lugar de utilizar la instancia Trac de Django o las listas de correo públicas.

Mas información:
https://www.djangoproject.com/weblog/2022/jul/04/security-releases