BOLETÍN DE ALERTA

Boletín Nro.: 2022-36
Fecha de publicación: 25/08/2022
Tema: Vulnerabilidad SQL Injection en Django

Productos afectados:

- Django, versiones 3.2 anteriores a 3.2.14.
- Django, versiones 4.0 anteriores a 4.0.6.

Descripción:

Se ha reportado un nuevo aviso de seguridad sobre una vulnerabilidad que afecta a varias versiones de Django, que permitiría a un atacante realizar consultas SQL arbitrarias en la base de datos.

La vulnerabilidad identificada como CVE-2022-34265, de severidad "Crítica" y con puntuación asignada de 9.8. Esta se debe a una falla en las funciones de bases de datos *Trunc(kind)* y *Extract(lookup_name).* Un atacante remoto podría ejecutar comandos *SQL* arbitrarios dentro de la base de datos de la aplicación, a través de la manipulación del parámetro kind/lookup_name de un input desconocido.

Actualmente para esta vulnerabilidad, existen PoC publicados en Internet.

Impacto:

La explotación exitosa de esta vulnerabilidad permitiría a un atacante ejecutar comandos SQL arbitrarios dentro de la base de datos y obtener el control total sobre la misma.

Solución:

Django recomienda actualizar a las versiones *3.2.x* y *4.0.x* respectivamente, a través de los siguientes enlaces:

- Django 3.2.x
- Django 4.0.x

Información adicional:

- https://www.cert.gov.py/noticias/vulnerabilidad-sql-injection-en-django/
- https://xz.aliyun.com/t/11628
- https://www.djangoproject.com/weblog/2022/jul/04/security-releases/
- https://security.snyk.io/vuln/SNYK-DEBIAN12-PYTHONDJANGO-2940826

- https://nvd.nist.gov/vuln/detail/CVE-2022-34265
- https://github.com/django/django/commit/54eb8a374d5d98594b264e8ec22337819b37443c
- https://github.com/django/django/commit/a9010fe5555e6086a9d9ae50069579400ef0685e