Alerta de seguridad informática	9VSA20-00152-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	09 de marzo de 2020
Última revisión	09 de marzo de 2020

NOTIFICACIÓN

La información consignada en el presente informe es producto del análisis de múltiples fuentes, de terceras partes, del propio fabricante e investigación propia del equipo CSIRT. La información contenida en los informes o comunicados está afecta a actualizaciones.

Resumen

El Equipo de Respuesta ante Incidentes de Seguridad Informática, CSIRT, comparte información obtenida del sitio oficial de Django, referente a una vulnerabilidad que afecta a su marco de desarrollo web, la cual permitiría a un atacante remoto realizar inyecciones SQL. Este informe incluye su respectiva mitigación.

Vulnerabilidad

CVE-2020-9402

Impacto

Un atacante remoto podría realizar inyecciones SQL en la base de datos de Django, permitiéndole leer, modificar, agregar y eliminar datos de esta y comprometiéndola completamente. Esta vulnerabilidad existe debido a la insuficiente sanitización de los datos entregados por el usuario si es que datos no confiables son utilizados como parámetro de confianza en funciones y agregados de GIS en Oracle.

Producto Afectado

Django 3.0.x, 2.2.x y 1.11.x.

Mitigación

Para la versión 1.11.x, actualizar a la versión 1.11.29.
Para la versión 2.2.x, actualizar a la versión 2.2.11.
Para la versión 3.0.x, actualizar a la versión 3.0.4.

Enlaces

https://www.djangoproject.com/weblog/2020/mar/04/security-releases/

https://docs.djangoproject.com/en/3.0/releases/security/

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-9402

CSIRT Gobierno de Chile

Firmado digitalmente por CSIRT Gobierno de Chile
Fecha: 2020.03.09 12:47:20 -03'00'