Alerta de seguridad informática	**9VSA-00028-001**
Clase de alerta	**Vulnerabilidad**
Tipo de incidente	**Sistema y/o Software Abierto**
Nivel de riesgo	**Alto**
TLP	**Blanco**
Fecha de lanzamiento original	**3 de Agosto de 2019**
Última revisión	**3 de Agosto de 2019**

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 la información entregada por Django (Framework de desarrollo web de código abierto) referente a múltiples vulnerabilidades que afectan a distintas versiones del software.

Vulnerabilidad

CVE-2019-14232
CVE-2019-14233
CVE-2019-14234
CVE-2019-14235

Impacto

CVE-2019-14232

La vulnerabilidad permite que un atacante remoto realice un ataque de denegación de servicio (DoS).

La vulnerabilidad existe debido al uso de filtros de plantilla truncatechars_html y truncatewords_html en django.utils.text.Truncator durante la evaluación del contenido HTML. Un atacante remoto puede pasar gran contenido en formato HTML a la aplicación y provocar el agotamiento de los recursos.

CVE-2019-14233

La vulnerabilidad permite que un atacante remoto realice un ataque de denegación de servicio (DoS).

La vulnerabilidad existe debido al uso de django.utils.html.strip_tags() durante la evaluación del contenido HTML. Un atacante remoto puede pasar gran contenido en formato HTML a la aplicación y provocar el agotamiento de los recursos.

CVE-2019-14234

La vulnerabilidad permite que un atacante remoto ejecute consultas SQL arbitrarias en la base de datos.

La vulnerabilidad existe debido a la limpieza insuficiente de los datos proporcionados por el usuario en django.contrib.postgres.fields.JSONField y django.contrib.postgres.fields.HStoreField. Un atacante remoto puede enviar una solicitud especialmente diseñada a la aplicación afectada y ejecutar comandos SQL arbitrarios dentro de la base de datos de la aplicación.

La explotación exitosa de esta vulnerabilidad puede permitir que un atacante remoto lea, elimine, modifique datos en la base de datos y obtenga un control completo sobre la aplicación afectada.

CVE-2019-14235

La vulnerabilidad permite que un atacante remoto realice un ataque de denegación de servicio (DoS).

La vulnerabilidad existe debido a un error al analizar los datos URF-8 con django.utils.encoding.uri_to_iri(). Un atacante remoto puede pasar contenido especialmente diseñado a la aplicación y consumir toda la memoria disponible en el sistema.

Productos Afectados

Django master development branch
Django 2.2 versiones anterior a 2.2.4
Django 2.1 versiones anterior a 2.1.11
Django 1.11 versiones anterior a 1.11.23

Mitigación

Instalar las actualizaciones liberadas por el fabricante directamente de su página web.

Enlace

https://www.djangoproject.com/weblog/2019/aug/01/security-releases/

CSIRT
Gobierno de
Chile

Firmado digitalmente
por CSIRT Gobierno de
Chile
Fecha: 2019.08.03
14:31:24 -04'00'