Alerta de seguridad informática	9VSA-00095-001
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	03 de diciembre de 2019
Última revisión	03 de diciembre 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 información obtenida del sitio oficial de Django, referente a una vulnerabilidad que afecta a su framework web, la cual, de ser explotada, puede resultar en escalación de privilegios. El informe incluye las actualizaciones para mitigar el riesgo.

Vulnerabilidad

CVE-2019-19118

Impacto

Es posible desencadenar una escalada de privilegios modificando los modelos principales de Django, a través de los modelos en línea. El usuario solo tiene permisos de lectura para el modelo principal, pero para el modelo en línea tiene permisos de edición. Con éste se actualiza al modelo principal y luego se llama al método save(), lo que provoca efectos secundarios, entre ellos, cargar gestores de señal previos y posteriores al guardado.

Producto Afectado

Las siguientes versiones de Djangoproject son vulnerables:

- 2.1
- 2.1.1
- 2.1.2
- 2.1.3
- 2.1.4
- 2.1.5
- 2.1.6
- 2.1.7
- 2.1.8
- 2.1.9
- 2.1.10
- 2.1.11
- 2.1.12
- 2.1.13
- 2.1.14
- 2.2
- 2.2.1
- 2.2.2
- 2.2.3
- 2.2.4
- 2.2.5
- 2.2.6
- 2.2.7

Mitigación

Para 2.1, actualizar a la versión 2.1.15
Para 2.2, actualizar a la versión 2.2.8.
Django también ha lanzado la versión 3.0 con esta vulnerabilidad mitigada.

Enlaces

- https://www.djangoproject.com/weblog/2019/dec/02/django-3-released/
- https://github.com/django/django/commit/11c5e0609bcc0db93809de2a08e0dc3d70b393e4
- https://cve.mitre.org/cgi-bin/cvename.cgi?name=2019-19118