Alerta de seguridad cibernética	9VSA20-00242-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	11 de junio de 2020
Última revisión	11 de junio 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 la información obtenida de Django referente a dos vulnerabilidades que afectan a su marco de desarrollo web. El presente informe incluye las respectivas medidas de mitigación.

Vulnerabilidades

CVE-2020-13254
CVE-2020-13596

Impactos

CVE-2020-13254
Debido a un error de validación de llave en "memcached backend", un atacante podría enviar una llave para el caché malformada resultando en la colisión de llaves y posible filtración de información.
Se implementó un validador de llaves al "memcache backend" para subsanar esta vulnerabilidad.

CVE-2020-13596
Debido a que el parametro para administrador "ForeignKeyRawIdWidget" no codifica correctamente las URLs, es posible para un atacante crear un enlace especialmente diseñado, enviarlo a una víctima para que acceda y realizar el ataque XSS (Cross-site scripting). Esto le permitiría al atacante modificar la apariencia del sitio web, robar información potencialmente sensible y engañar al usuario para que descargue malware.
Se corrigió la codificación URL en el parámetro afectado para subsanar esta vulnerabilidad.

Productos Afectados
Django rama maestra.
Django versión 3.1 (En estado alpha).
Django versión 3.0.
Django versión 2.2.

Mitigación
Se deben aplicar las actualizaciones publicadas en el git oficial o sitio oficial de Django.

Enlaces
https://docs.djangoproject.com/en/3.0/releases/security/
https://www.djangoproject.com/weblog/2020/jun/03/security-releases/
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-13254
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-13596