Basque CyberSecurity Centre

Vulnerabilidad crítica en Django

BCSC-AVISOS

TLP: CLEAR

www.ciberseguridad.eus

EUSKO JAURLARITZA GOBIERNO VASCO

GRUPO spri TALDEA

TABLA DE CONTENIDO

Cláusula de exención de responsabilidad

El presente documento se proporciona con el objeto de divulgar las alertas que el BCSC considera necesarias en favor de la seguridad de las organizaciones y de la ciudadanía interesada. En ningún caso el BCSC puede ser considerado responsable de posibles daños que, de forma directa o indirecta, de manera fortuita o extraordinaria pueda ocasionar el uso de la información revelada, así como de las tecnologías a las que se haga referencia tanto de la web de BCSC como de información externa a la que se acceda mediante enlaces a páginas webs externas, a redes sociales, a productos de software o a cualquier otra información que pueda aparecer en la alerta o en la web de BCSC. En todo caso, los contenidos de la alerta y las contestaciones que pudieran darse a través de los diferentes correos electrónicos son opiniones y recomendaciones acorde a los términos aquí recogidos no pudiendo derivarse efecto jurídico vinculante derivado de la información comunicada.

Cláusula de prohibición de venta

Queda terminantemente prohibida la venta u obtención de cualquier beneficio económico, sin perjuicio de la posibilidad de copia, distribución, difusión o divulgación del presente documento.

Sobre el BCSC

El Centro Vasco de Ciberseguridad (Basque Cybersecurity Centre, BCSC) es la entidad designada por el Gobierno Vasco para elevar el nivel de madurez de la ciberseguridad en Euskadi.

Es una iniciativa transversal que se enmarca en la Agencia Vasca de Desarrollo Empresarial (SPRI), sociedad dependiente del Departamento de Desarrollo Económico, Sostenibilidad y Medio Ambiente del Gobierno Vasco. Así mismo, involucra a otros tres Departamentos del Gobierno Vasco: el de Seguridad, el de Gobernanza Pública y Autogobierno, y el de Educación, y a cuatro agentes de la Red Vasca de Ciencia, Tecnología e Innovación: Tecnalia, Vicomtech, Ikerlan y BCAM.

El BCSC es la entidad de referencia para el desarrollo de la ciberseguridad y de la confianza digital de ciudadanos, empresas e instituciones públicas en Euskadi, especialmente para los sectores estratégicos de la economía de la región.

La misión del BCSC es por tanto promover y desarrollar la ciberseguridad en la sociedad vasca, dinamizar la actividad empresarial de Euskadi y posibilitar la creación de un sector profesional que sea referente. En este contexto se impulsa la ejecución de proyectos de colaboración entre actores complementarios en los ámbitos de innovación tecnológica, investigación y transferencia tecnológica a la industria de fabricación avanzada y otros sectores.

Así mismo, ofrece diferentes servicios en su rol como Equipo de Repuesta a Incidentes (en adelante CERT, por sus siglas en inglés “Computer Emergency Response Team”) y trabaja en el ámbito de la Comunidad Autónoma del País Vasco para aumentar la capacidad de detección y alerta temprana de nuevas amenazas, la respuesta y análisis de incidentes de seguridad de la información, y el diseño de medidas preventivas para atender a las necesidades de la sociedad vasca. Con el fin de alcanzar estos objetivos forma parte de diferentes iniciativas orientadas a la gestión de incidentes de ciberseguridad:

FIRST Improving Security Together
TF-CSIRT Trusted Introducer
CSIRT.es

1. Aviso de seguridad

Se ha actualizado el estado de una vulnerabilidad publicada en un aviso de seguridad el pasado 3 de mayo de 2023 que afecta al framework de desarrollo web Django. La vulnerabilidad, cuyo identificador es CVE-2023-31047, es un fallo crítico de bypass en la validación de formularios y cuya explotación exitosa supondría un alto impacto sobre la confidencialidad, integridad y disponibilidad de los sistemas afectados.

El fabricante ya ha publicado la actualización correspondiente corrigiendo de esta manera el fallo destacado, por lo que, para prevenir estas y otras vulnerabilidades, se recomienda tener siempre los sistemas y aplicaciones actualizadas a la última versión disponible.

2. Recursos afectados

- Django 3.2 versiones anteriores a la 3.2.19.
- Django 4.0 versiones anteriores a la a 4.1.9.
- Django 4.2 versiones anteriores a la 4.2.1.

3. Análisis técnico

El detalle de la vulnerabilidad abordada en esta actualización es el siguiente:

CVE-2023-31047: vulnerabilidad de bypass en la validación de formularios, de manera que, la carga de varios archivos usando un campo de formulario no es compatible con *forms.FileField* o *Forms.ImageField*, ya que solo se valida el último archivo cargado. Para evitar el error, los widgets de formulario *ClearableFileInput* y *FileInput* ahora generan un *ValueError* cuando se establece el atributo HTML múltiple en ellos. Para evitar la excepción y mantener el comportamiento anterior, se recomienda establecer *allow_multiple_selected* a True.

La métrica de evaluación de la vulnerabilidad se compone de:

CWE 20: Improper Input Validation

CVSS Base: 9.8

CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

- **Vector de ataque**: **Red**
- **Complejidad del ataque**: **Baja**
- **Privilegios requeridos: Ningunos**
- **Interacción con el usuario**: **Ninguna**
- **Alcance**: Sin cambios
- **Confidencialidad: Alta**
- **Integridad: Alta**
- **Disponibilidad: Alta**

4. Mitigación / Solución

Para la mitigación de estas vulnerabilidades, se recomienda tener siempre los sistemas y aplicaciones actualizadas a la última versión disponible en cuanto se publiquen las actualizaciones correspondientes.

Para tratar la vulnerabilidad descrita, Django ha publicado actualizaciones para el framework disponibles en los siguientes enlaces:

- Mitigación para Django 4.2.
- Mitigación para Django 4.1.
- Mitigación para Django 3.2.

5. Referencias Adicionales

- Aviso de seguridad.
- CVE-2023-31047.

EUSKO JAURLARITZA GOBIERNO VASCO
GRUPO spri TALDEA