Alerta de seguridad informática	9VSA-00104-001
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	19 de diciembre de 2019
Última revisión	19 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 entregada por Django referente a una vulnerabilidad que afecta su marco de desarrollo de aplicaciones web. El informe también contiene los enlaces para descargar las respectivas mitigaciones.

Vulnerabilidad

CVE-2019-19844

Impacto

Secuestro de cuenta.
Un atacante puede robar cuentas explotando una vulnerabilidad en la función “restablecer contraseña”. Cuando un usuario necesita restablecer la cuenta, Django solicita un correo para enviar un token de recuperación de contraseña. Al hacerlo, la cuenta ingresada por el usuario se contrasta con la base de datos de Django. El sistema, al no sanitizar correctamente la comparación de las cuentas, transformará ambas cuentas a formato Unicode. Un atacante podría explotar la vulnerabilidad generando un correo falso que, al ser convertido a Unicode, puede ser interpretado como equivalente al correo en la base de datos. Al asumir que el correo ingresado es válido, enviara a éste último el token de recuperación.

Productos Afectados

Django versiones 1.11.26, 2.2.8 y 3.0 y Master Branch.

Mitigación

Actualizar a la versión 1.11.27, 2.2.9 ó 3.0.1 de Django.

Enlaces

https://www.djangoproject.com/weblog/2019/dec/18/security-releases/
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-19844

CSIRT Gobierno de Chile
Firmado digitalmente por CSIRT Gobierno de Chile
Fecha: 2019.12.19 17:37:02 -03'00'