BOLETÍN DE ALERTA

Boletín Nro.: 2017-02
Fecha de publicación: 20/04/2017
Tema: Vulnerabilidad crítica en Drupal

Sistemas afectados:

- Todas las versiones Drupal 8.x

Descripción:

Se ha reportado una vulnerabilidad crítica de bypass de control de acceso que afecta a todas las versiones de Drupal de la rama 8, identificada como CVE-2017-6919. Esta vulnerabilidad es explotable en aquellos sitios que cumplan las siguientes condiciones:

- Tienen habilitado el módulo RESTful Web Services (rest)
- Permite solicitudes PATCH
- Permite registro de usuarios y/o se compromete una cuenta de usuario

La rama Drupal 7.x no está afectada por esta vulnerabilidad.

Para corregir esta vulnerabilidad, Drupal ha publicado una actualización en la versión 8.3.1 y 8.2.8. Debido a la criticidad de esta vulnerabilidad, Drupal ha publicado un parche incluso para aquellas versiones afectadas que ya no tienen soporte.

Impacto

Explotando esta vulnerabilidad un atacante remoto no autorizado podría obtener un control total del servidor que aloja la aplicación de Drupal vulnerable.

Solución

Drupal ha publicado una actualización, Drupal 8.3.1 la cual corrige las vulnerabilidades. También ha publicado una actualización 8.2.8 para aquellos sitios que no habían actualizado a 8.3, sin embargo, se

CERT-PY Equipo de Respuestas ante Emergencias Cibernéticas
Secretaría Nacional de Tecnologías de la Información y Comunicación (SENATICs)
Gral. Santos y Concordia – Complejo Santos – Ofic. E14
cert@cert.gov.py | +595 21 201014 | +595 21 3276902
Asunción - Paraguay | www.cert.gov.py
@CERTpy
/CERT-Py

recomienda, luego de aplicar el parche, actualizar a ésta, ya que 8.2.x se encuentra ya sin soporte. Se recomienda actualizar los sitios afectados de inmediato. La nueva versión puede ser obtenida aquí:

Drupal 8.3.1: https://www.drupal.org/project/drupal/releases/8.3.1

Drupal 8.2.8: https://www.drupal.org/project/drupal/releases/8.2.8

Puede leer la guía oficial de actualización de Drupal aquí:

https://www.drupal.org/docs/7/updating-your-drupal-site/how-to-update-drupal-core

Información adicional:

https://www.drupal.org/SA-CORE-2017-002

CERT-PY Equipo de Respuestas ante Emergencias Cibernéticas
Secretaría Nacional de Tecnologías de la Información y Comunicación (SENATICs)
Gral. Santos y Concordia – Complejo Santos – Ofic. E14
cert@cert.gov.py | +595 21 201014 | +595 21 3276902
Asunción - Paraguay | www.cert.gov.py
@CERTpy
/CERT-Py