Drupal , Seguridad De Contraseña

Drupal Soluciona Grave Fallo De Seguridad De Contraseña

Drupal, uno de los **sistema de gestión de contenido de código abierto** ampliamente utilizado está recomendando a sus usuarios actualizar su software a las últimas versiones 6.35 y 7.35, después que la compañía descubrió dos vulnerabilidades moderadamente críticas que pueden permitir a un atacante **hackear sitios web en Drupal**.

De acuerdo con un aviso de seguridad publicado, un fallo que se encuentra en el **núcleo de Drupal** podría permitir a un hacker eludir restricciones de seguridad en determinadas circustancias, forjando el restablecimiento de contraseñas.

Acceso BYPASS Y Vulnerabilidad Del Restablecimiento De Contraseñas

Una explotación exitosa de esta vulnerabilidad con acceso Bypass podría aprovechar el hacker para obtener acceso no autorizado a cuentas de usuario **sin conocer la contraseña**.

Esta vulnerabilidad se considera como moderadamente crítica,

ya que un atacante puede engañar a un usuario registrado del sitio web basado en Drupal, como administrador, en el lanzamiento de una URL creada con fines malintencionados en un intento de tomar el control del servidor de destino.

Sitios Web Con Drupal Afectados

La explotación de la vulnerabilidad de acceso de bypass en Drupal 7, es posible sólo si la cuenta de importada o editada de los resultados del proceso en el hash de la contraseña en la base de datos, es la misma para múltiples cuentas de usuario.

Los sitios web que ejecutan Drupal 6 están en mayor riesgo, debido a que los administradores de los sitios web se han creado varias nuevas cuentas de usuario protegidas por la misma contraseña.

Por otra parte, la vulnerabilidad de la seguridad también puede ser explotada en los sitios web con Drupal 6, donde las cuentas se han importado o editadosde manera que resulte en el campo hash de la contraseña en la base de datos esté vacía, por lo menos para una cuenta de usuario.

> *«Los sitios en Drupal 6, que tienen los hashes de contraseñas vacías, o un campo de contraseña con una cadena fácil de*

> *adivinar en la base de datos, son especialmente propensos a esta vulnerabilidad,» las notas de asesoramiento de seguridad de Drupal. «Esto podría aplicarse a los sitios que utilizan la autenticación externa para que el campo de contraseña se establezca en un valor no válido fijo.»*

Vulnerabilidad REDIRECT OPEN

Las **versiones afectadas del CMS Drupal**, también son susceptibles a una vulnerabilidad de redirección abierta. La URL de acción en Drupal, contiene un parámetro de «destino» en él, que puede ser utilizado por los ciberdelincuentes para redirigir a los usuarios a un sitio de terceros con contenido malicioso.

Según el equipo de Drupal, hay múltiples funciones de la API relacionados con la URL en versiones afectadas de Drupal 6 y 7 que pueden ser utilizados por los atacantes en pasar a través de URLs externas cuando no es necesario. Esto podría dar lugar a vulnerabilidades de redirección abiertas adicionales.

> *«Esta vulnerabilidad se ve mitigado por el hecho de que muchos de los usos comunes del parametro de destino no son susceptibles al ataque», señalan los desarrolladores. «Sin embargo, todas las formas de confirmación desarrolladas utilizando la API del formulario de Drupal 7 son vulnerables a través de la acción Cancelar que aparece en la parte inferior del formulario, y algunos Drupal 6 formas de confirmación son vulnerables también.»*

La cuestión es realmente grave porque Drupal se usa en cerca de 1 billón de sitios web en Internet, lo que pone a Drupal en el tercer lugar detrás de WordPress y Joomla. Drupal proporciona un sistema de gestión de contenido para sitios web, entre los cuales se encuentran MTV, Popular Science, Sony Music, Harvard y MIT.