El equipo de desarrollo de Drupal lanzó ayer actualizaciones importantes de seguridad para su software de gestión de contenido, de código abierto, ampliamente utilizado, para abordar una vulnerabilidad crítica y tres vulnerabilidades *«moderadamente críticas»* en su sistema central.

Tomando en cuenta que los sitios web con tecnología de Drupal se encuentran entre los objetivos favoritos de todos los tiempos para los piratas informáticos, se recomienda a los administradores del sitio web que instalen la última versión de Drupal 7.69, 8.711 o 8.8.1, para evitar que los hackers remotos comprometan los servidores web.

El único aviso con gravedad crítica incluye parches para múltiples vulnerabilidades en una biblioteca de terceros, llamada *«Archive_Tar»*, que Drupal Core usa para crear, enumerar, extraer y agregar archivos a contenedores Tar.

La vulnerabilidad reside en la forma en que la biblioteca afectada descomprime los archivos con enlaces simbólicos, que si se explotan, podrían permitir que un atacante sobrescriba archivos confidenciales en un servidor de destino al cargar un archivo tar creado con fines malintencionados.

Debido a esto, se debe notar que la falla solo afecta a los sitios web de Drupal que están configurados para procesar archivos .tar, .tar.gz, .bz2 o .tlz cargados por usuarios no confiables.

Según los desarrolladores de Drupal, ya existe un exploit de prueba de concepto para esta vulnerabilidad y, teniendo en cuenta la popularidad de los exploits de Drupal entre los piratas informáticos, es posible que los piratas informáticos exploten activamente este defecto en la naturaleza para atacar los sitios web de Drupal.

Vulnerabilidades moderadamente críticas

Además de la vulnerabilidad crítica, los desarrolladores de Drupal también parchearon tres vulnerabilidades *«moderadamente críticas»*, cuyos detalles se enlistan a continuación.

- Denegación de servicio (DoS): el archivo install.php utilizado por Drupal 8 Core contiene una falla que puede ser explotada por un atacante remoto no autenticado para perjudicar la disponibilidad de un sitio web objetivo al corromper sus datos almacenados en caché.
- Bypass de restricción de seguridad: la función de carga de archivos en Drupal 8 no elimina los puntos iniciales y finales de los nombres de archivos, que pueden ser utilizados por un atacante con capacidad de carga de archivos para sobrescribir archivos arbitrarios del sistema, como .htaccess para omitir las protecciones de seguridad.
- Acceso no autorizado: esta vulnerabilidad existe en el módulo predeterminado de la biblioteca de medios de Drupal cuando no restringe correctamente el acceso a los elementos de medios en ciertas configuraciones. Por lo tanto, podría permitir que un usuario con pocos privilegios obtenga acceso no autorizado a información confidencial que de otra forma estaría fuera de su alcance.

Según los desarrolladores, los administradores de sitios web afectados pueden mitigar la vulnerabilidad de omisión de medios de acceso al desmarcar la casilla de verificación *«Habilitar IU avanzada»* en /admin/config/media/media-library, aunque esta mitigación no está disponible en versiones 8.7.x.

Todas las vulnerabilidades «moderadamente críticas» anteriores se han parcheado con el lanzamiento de las versiones de Drupal 8.7.11 y 8.8.1, y hasta ahora, no se ha ejecutado ninguna prueba de concepto para estas vulnerabilidades.

Debido a que existe una prueba de concepto para la vulnerabilidad crítica de Drupal, se recomienda a los usuarios que ejecutan versiones vulnerables, que actualicen su CMS a la última versión principal de Drupal lo más pronto posible.