I. DATOS GENERALES:

Clase de alerta: Vulnerabilidad

Tipo de incidente: Acceso no autorizado

Nivel de riesgo: Medio

II. ALERTA

Figura 1.- Drupal core - Access bypass - SA-CORE-2023-005

La función de descarga de archivos no evade suficientemente las rutas de los archivos en ciertas situaciones. *Esto puede dar lugar a que los usuarios obtengan acceso a archivos privados a los que no deberían tener acceso.*

Algunos sitios pueden requerir cambios de configuración después de esta versión de seguridad. Revise las notas de la versión de su versión de Drupal si tiene problemas para acceder a los archivos privados después de la actualización.

Este aviso está cubierto por Drupal Steward. Debido a que esta vulnerabilidad no es explotable en masa, su socio Steward puede responder solo monitoreando, en lugar de hacer cumplir una nueva regla WAF.

Drupal 7

Todos los sitios de Drupal 7 en servidores web de Windows son vulnerables.

Los sitios de Drupal 7 en servidores web Linux son vulnerables con ciertas estructuras de directorio de archivos, o si se instala un módulo de acceso a archivos personalizado o contribuido vulnerable.

Drupal 9 y 10

Los sitios de Drupal 9 y 10 solo son vulnerables si se instalan ciertos módulos de acceso a archivos personalizados o contribuidos.

Fuente: https://www.drupal.org/sa-core-2023-005

III. INTRODUCCIÓN

Drupal es un software de gestión de contenidos. Se usa para hacer muchos de los sitios web y aplicaciones que usa todos los días. Drupal tiene excelentes funciones estándar, como la creación de contenido fácil, un rendimiento confiable y una seguridad excelente. Pero lo que lo distingue es su flexibilidad; lamodularidad es uno de sus principios fundamentales. Sus herramientas lo ayudan a crear el contenido versátil y estructurado que necesitan las experiencias web dinámicas. (Fuente: https://www.drupal.org/about)

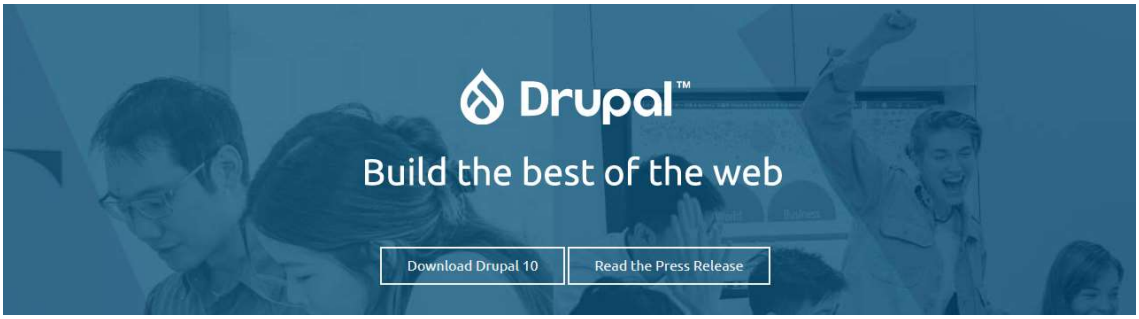

Figura 2. Drupal 10
Fuente: https://www.drupal.org/about/10

Referente a la "Omisión de acceso en el core de Drupal", la explotación de esta vulnerabilidad podría dar lugar a que los usuarios obtengan acceso a archivos privados a los que no deberían tenerlo.

La vulnerabilidad detectada provoca que la función de descarga de archivos no depure las rutas de estos en ciertas situaciones. Esto puede dar lugar a que los usuarios obtengan acceso a archivos privados a los que no deberían tener acceso.

Los recursos afectados podrían ser: (Fuente: https://www.incibe.es/incibe-cert/alerta-temprana/avisos/omision-de-acceso-en-el-core-de-drupal)

- Servidores web de Windows y Linux, versión 7.
- Ciertos módulos de acceso a archivos personalizados o contribuido en versiones 9 y 10.

IV. VECTOR DE ATAQUE:

Sistema vulnerable

V. IMPACTO:

CI - Impacto de la confidencialidad: ¿Esta vulnerabilidad hace que los datos no públicos sean accesibles?	**CI: Algunos =** Ciertos datos no públicos se publican
II - Impacto de integridad: ¿Puede este exploit permitir que los datos del sistema (o los datos manejados por el sistema) se vean comprometidos?	**II: Ninguno** = La integridad de los datos permanece intacta

E: Explotación (impacto de día cero): ¿Existe un exploit conocido?	**E: Teórico** = Teórico o sombrero blanco (no existe ningún código de explotación pública ni documentación sobre el desarrollo)

VI. INDICADORES DE COMPROMISO

CVE – ID: CVE-2023-31250

VII. RECOMENDACIONES:

El EcuCERT recomienda a su comunidad objetivo tomar en consideración lo siguiente:

- Instale la última versión para el software de gestión de contenidos, Drupal.
  - Si está utilizando Drupal 10.0, actualice a Drupal 10.0.8.
  - Si está utilizando Drupal 9.5, actualice a Drupal 9.5.8.
  - Si está utilizando Drupal 9.4, actualice a Drupal 9.4.14.
  - Si está utilizando Drupal 7, actualice a Drupal 7.96.
  - Todas las versiones de Drupal 9 anteriores a 9.4.x están al final de su ciclo de vida y no reciben cobertura de seguridad. Tenga en cuenta que Drupal 8 ha llegado al final de su vida útil.
- Instalar actualizaciones disponibles en medios oficiales del proveedor, previo análisis del impacto que podría provocar en los servicios críticos para el negocio de la organización.
- Realizar copias de respaldo de seguridad periódicas, de la información crítica para evitar la pérdida de la misma.
- Actualizar el sistema operativo de los equipos a las últimas versiones.
- No abrir, manipular, o interactuar, con correos electrónicos altamente sospechosos que lleguen a las bandejas de correo o mensaje en redes sociales.
- Otorgar privilegios de usuario al mínimo dependiendo del tipo de labor a realizar.
- Implementar técnicas de navegación segura en toda la Institución/Organización, como por ejemplo visita únicamente de sitios con certificados SSL, y, de origen no sospechoso.
- Bloquear el acceso de usuarios, a dispositivos de almacenamiento externo, ajenos a la Institución/Organización, a través de políticas de seguridad adecuadas.

- Implementar y monitorear, plataformas de seguridad perimetral para identificar posible tráfico malicioso tanto a nivel interno como externo a la infraestructura de red de la organización/Institución
- Descargar programas, archivos y actualizaciones, solamente desde fuentes oficiales y verificadas.
- Cerrar todo tipo de conexión/protocolo de acceso remoto a infraestructuras críticas en la Organización/Institución, en el caso de requerir su implementación, realizarlo bajo estrictas normas de seguridad apalancados en plataformas de seguridad perimetral y, uso de una VPN.
- Tener actualizado y utilizar, un software anti-virus
- Mantener actualizados, y, bajo licenciamiento, (ya sea a nivel de software libre o de paga, de ser el caso), todos y cada uno de los sistemas y subsistemas de software y hardware de toda la infraestructura de IT y OT de la Institución, esto es, incluido a nivel de Firmware de todos los componentes.
- Diseñar una política de revisión de logs, que permita detectar comportamientos fuera de lo normal en procesos legítimos del sistema.
- Mantener listas de control de acceso para las unidades mapeadas en red restringiendo los privilegios de escritura. Con esto podrá identificar el impacto generado por el cifrado de archivos, entendiendo que el secuestro de información se producirá en todas las unidades de red mapeadas en el equipo víctima.
- Capacitar a todos los usuarios, mediante la concientización y simulaciones para reconocer e informar sobre intentos de phishing e ingeniería social. Seguir las normativas internacionales tales como ISO 27001:2013 en su control A.7.2.2 “Concienciación con educación y capacitación en seguridad de la información” o NIST PR.AT-1: “Todos los usuarios se encuentran entrenados e informados”, a fin de tener bases para divulgar campañas educativas orientadas a nivel de usuarios respecto al correcto uso de las herramientas tecnológicas
- Implementar un plan de respuesta a emergencias de la Organización/Institución.
- En el caso de sufrir un ataque de proporciones mayores, contacte a las Autoridades competentes en base a la Normativa Legal Vigente a nivel Nacional.

VIII. DESCARGO DE RESPONSABILIDAD

- La información en la presente alerta; se proporciona con fines informativos.
- Cualquier referencia a productos, procesos o servicios comerciales específicos, no constituye respaldo o recomendación por parte del EcuCERT a los mismos.
- La presente alerta no debe utilizarse con fines publicitarios o de patrocinio de productos.

IX. REFERENCIAS:

Drupal (2023). *Security risk levels defined.*, recuperado de https://www.drupal.org/drupal-security-team/security-risk-levels-defined

- **Drupal (2023).** *Drupal core - Moderately critical - Access bypass - SA-CORE-2023-005.*, recuperado de https://www.drupal.org/sa-core-2023-005
- **INCIBE-CERT (2023).** *Omisión de acceso en el core de Drupal*, recuperado de https://www.incibe.es/incibe-cert/alerta-temprana/avisos/omision-de-acceso-en-el-core-de-drupal
- **CCN-CERT (2023).** *Boletines de Vulnerabilidades – Drupal core – Moderality critical – Access bypass – SA-CORE-2023-005.*, recuperado de https://www.ccn-cert.cni.es/ca/component/vulnerabilidades/view/34256.html?search=act