Basque CyberSecurity Centre

Vulnerabilidades críticas en módulos de Drupal

BCSC-AVISOS

TLP: CLEAR

www.ciberseguridad.eus

EUSKO JAURLARITZA GOBIERNO VASCO

GRUPO spri TALDEA

TABLA DE CONTENIDO

Cláusula de exención de responsabilidad

El presente documento se proporciona con el objeto de divulgar las alertas que el BCSC considera necesarias en favor de la seguridad de las organizaciones y de la ciudadanía interesada. En ningún caso el BCSC puede ser considerado responsable de posibles daños que, de forma directa o indirecta, de manera fortuita o extraordinaria pueda ocasionar el uso de la información revelada, así como de las tecnologías a las que se haga referencia tanto de la web de BCSC como de información externa a la que se acceda mediante enlaces a páginas webs externas, a redes sociales, a productos de software o a cualquier otra información que pueda aparecer en la alerta o en la web de BCSC. En todo caso, los contenidos de la alerta y las contestaciones que pudieran darse a través de los diferentes correos electrónicos son opiniones y recomendaciones acorde a los términos aquí recogidos no pudiendo derivarse efecto jurídico vinculante derivado de la información comunicada.

Cláusula de prohibición de venta

Queda terminantemente prohibida la venta u obtención de cualquier beneficio económico, sin perjuicio de la posibilidad de copia, distribución, difusión o divulgación del presente documento.

Sobre el BCSC

El Centro Vasco de Ciberseguridad (Basque Cybersecurity Centre, BCSC) es la entidad designada por el Gobierno Vasco para elevar el nivel de madurez de la ciberseguridad en Euskadi.

Es una iniciativa transversal que se enmarca en la Agencia Vasca de Desarrollo Empresarial (SPRI), sociedad dependiente del Departamento de Desarrollo Económico, Sostenibilidad y Medio Ambiente del Gobierno Vasco. Así mismo, involucra a otros tres Departamentos del Gobierno Vasco: el de Seguridad, el de Gobernanza Pública y Autogobierno, y el de Educación, y a cuatro agentes de la Red Vasca de Ciencia, Tecnología e Innovación: Tecnalia, Vicomtech, Ikerlan y BCAM.

El BCSC es la entidad de referencia para el desarrollo de la ciberseguridad y de la confianza digital de ciudadanos, empresas e instituciones públicas en Euskadi, especialmente para los sectores estratégicos de la economía de la región.

La misión del BCSC es por tanto promover y desarrollar la ciberseguridad en la sociedad vasca, dinamizar la actividad empresarial de Euskadi y posibilitar la creación de un sector profesional que sea referente. En este contexto se impulsa la ejecución de proyectos de colaboración entre actores complementarios en los ámbitos de innovación tecnológica, investigación y transferencia tecnológica a la industria de fabricación avanzada y otros sectores.

Así mismo, ofrece diferentes servicios en su rol como Equipo de Repuesta a Incidentes (en adelante CERT, por sus siglas en inglés “Computer Emergency Response Team”) y trabaja en el ámbito de la Comunidad Autónoma del País Vasco para aumentar la capacidad de detección y alerta temprana de nuevas amenazas, la respuesta y análisis de incidentes de seguridad de la información, y el diseño de medidas preventivas para atender a las necesidades de la sociedad vasca. Con el fin de alcanzar estos objetivos forma parte de diferentes iniciativas orientadas a la gestión de incidentes de ciberseguridad:

FIRST Improving Security Together
TF-CSIRT Trusted Introducer
CSIRT.es

1. Aviso de seguridad

Drupal ha publicado varios avisos de seguridad donde 4 de ellos, sa-contrib-2023-034, sa-contrib-2023-035, sa-contrib-2023-036 y sa-contrib-2023-038, corrigen vulnerabilidades críticas que afectan a los módulos ACL, Forum Access, Flexi Access y Shorthand. La explotación de la mayoría de estos errores produce un impacto de alta gravedad en la confidencialidad e integridad de los sistemas que se vean afectados.

El fabricante ya ha publicado las actualizaciones correspondientes, corrigiendo de esta manera los fallos destacados.

2. Recursos afectados

- Drupal 7 y 8.

3. Análisis técnico

En el aviso sa-contrib-2023-034 se corrige un fallo de severidad crítica en el módulo ACL, abreviatura de listas de control de acceso, una API para que otros módulos creen listas de usuarios y les den acceso a nodos. El módulo procesa la entrada del usuario de una manera que podría resultar insegura lo que puede conducir a la ejecución remota de código mediante inyección de objetos. Como se trata de un módulo API, sólo se puede explotar si un módulo "cliente" expone la vulnerabilidad.

La métrica de evaluación de la vulnerabilidad se compone de:

AC:Basic/A:Admin/CI:All/II:All/E:Theoretical/TD:All

- **Complejidad de acceso: Básica**
- **Autentificación:** Administrador
- **Impacto en la confidencialidad: Alto**
- **Impacto en la integridad: Alto**
- **Exploit:** Teórico, sin exploit publicado
- **Distribución objetivo: Todas las configuraciones del módulo son explotables.**

En el aviso sa-contrib-2023-035 se soluciona una vulnerabilidad en el módulo Forum Access que cambia la página de administración de un foro para permitir configurar los foros como privados. También controla qué roles de usuario pueden ver, editar, eliminar y publicar en cada foro y puede darle a cada foro una lista de usuarios que tienen acceso administrativo en ese foro. Este módulo requiere el módulo ACL. El módulo procesa la entrada del usuario de una manera que podría resultar insegura. Esto puede conducir a la ejecución remota de código mediante inyección de objetos. Esta vulnerabilidad se ve mitigada por el hecho de que un atacante necesita el permiso administrar foros.

La métrica de evaluación de la vulnerabilidad se compone de:

AC:Basic/A:Admin/CI:All/II:All/E:Theoretical/TD:All

- **Complejidad de acceso: Básica**
- **Autentificación:** Administrador
- **Impacto en la confidencialidad: Alto**
- **Impacto en la integridad: Alto**
- **Exploit:** Teórico, sin exploit publicado
- **Distribución objetivo: Todas las configuraciones del módulo son explotables.**

En el aviso sa-contrib-2023-036 se corrige un error en el módulo Flexi Access que proporciona una interfaz para el módulo ACL permitiendo configurar y

administrar ACL. El módulo procesa la entrada del usuario de una manera que podría resultar insegura. Esto puede conducir a la ejecución remota de código mediante inyección de objetos. Esta vulnerabilidad se ve mitigada por el hecho de que las rutas de explotación conocidas requieren que un atacante tenga una combinación de permisos proporcionados por el módulo.

La métrica de evaluación de la vulnerabilidad se compone de:

AC:Basic/A:Admin/CI:All/II:All/E:Theoretical/TD:All

- **Complejidad de acceso: Básica**
- **Autentificación:** Administrador
- **Impacto en la confidencialidad: Alto**
- **Impacto en la integridad: Alto**
- **Exploit:** Teórico, sin exploit publicado
- **Distribución objetivo: Todas las configuraciones del módulo son explotables.**

Por último para el aviso sa-contrib-2023-038 se corrige un fallo en el módulo que proporciona integración con Shorthand. El módulo no verifica los permisos apropiados al mostrar una lista de todas las historias breves.

La métrica de evaluación de la vulnerabilidad se compone de:

AC:None/A:None/CI:Some/II:None/E:Theoretical/TD:All

- **Complejidad de acceso: Ninguno**
- **Autentificación: Ninguno**
- **Impacto en la confidencialidad: Medio**
- **Impacto en la integridad:** Ninguno
- **Exploit:** Teórico, sin exploit publicado
- **Distribución objetivo: Todas las configuraciones del módulo son explotables.**

4. Mitigación / Solución

Para la mitigación de estas vulnerabilidades, se recomienda tener siempre los sistemas y aplicaciones actualizadas a la última versión disponible en cuanto se publiquen las actualizaciones correspondientes.

Para la mitigación del fallo de aviso sa-contrib-2023-034 desde Drupal se recomienda:

- Si utiliza el módulo ACL para Drupal 7.x, actualizar a ACL 7.x-1.4.
- Si utiliza el módulo ACL 8.x-1.0-beta3 o inferior, actualizar a ACL 8.x-1.0.

En cuanto a la vulnerabilidad tratada en el aviso sa-contrib-2023-035 Drupal recomienda:

- Si utiliza el módulo Forum Access para Drupal 7.x, actualizar a Forum Access 7.x-1.6.
- Si utiliza el módulo Forum Access 8.x-1.0-beta3 o inferior, actualizar a Forum Access 8.x-1.0.

Para el aviso sa-contrib-2023-036 las medidas a tomar son:

- Si utiliza el módulo Flexi Access para Drupal 7.x, actualizar a Flexi Access 7.x-1.3. El módulo ACL también debe actualizarse.

Por último, para el aviso sa-contrib-2023-038:

- Si se utiliza el módulo Shorthand para Drupal 8+, actualizar a Shorthand 4.0.3.

5. Referencias Adicionales

- Avisos de seguridad.
- sa-contrib-2023-034
- sa-contrib-2023-035.
- sa-contrib-2023-036.
- sa-contrib-2023-038.
- ACL.
- Forum Access.
- Flexi Access.
- Shorthand.


Basque
CyberSecurity
Centre


EUSKO JAURLARITZA
GOBIERNO VASCO


GRUPO
spri
TALDEA