BOLETÍN DE ALERTA

Boletín Nro.: 2016-09
Fecha de publicación: 20/06/2016
Tema: Vulnerabilidades críticas en Liferay y Drupal

Sistemas afectados:

Drupal:

- Drupal de la rama 7.x - todas las versiones previas a la 7.44
- Drupal de la rama 8.x - todas las versiones previas a la 8.1.3

Liferay:

- Versiones de Liferay Portal 6.2 CE GA6 sin parchear
- Versión 7.0.0 de Liferay Portal (7.0 CE GA1)

Descripción:

Se han reportado múltiples vulnerabilidades críticas y medias que afectan a dos CMS (*Content Management Systems*) populares: Drupal y Liferay.

En el caso de Drupal, se han reportado dos vulnerabilidades, clasificadas como moderadamente críticas. La primera de ellas afecta al módulo de usuarios de Drupal 7 debido a que al guardar bajo determinadas condiciones se pueden asignar a un usuario todos los roles del sitio, lo que podría permitir a un usuario conseguir permisos administrativos. Esta vulnerabilidad se encuentra mitigada por el hecho de que requiere código personalizado que fuerce al formulario de registro a reconstruirse al vuelo durante el envío del formulario de perfil de usuario.

La segunda vulnerabilidad, menos crítica, afecta al módulo de Vistas de Drupal 7 y 8 que podría permitir a usuarios sin autorización visualizar información del módulo de estadísticas. En Drupal 7 no afecta al Core, pero si se usa el modulo Vistas de Drupal 7.x, se debe actualizar este módulo a la versión Views 7.x-3.14.

En el caso de Liferay, se han publicado múltiples vulnerabilidades críticas que afectan a las versiones 6.2 CE GA6 y 7.0 CE GA1 del gestor de contenidos. Las vulnerabilidades más críticas que afectan a la versión 6.2 son las siguientes:

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

- Ejecución de código remoto y escalado de privilegios en las plantillas Velocity y FreeMarker
- La autenticación mediante digest no respeta la política de contraseñas, permitiendo múltiples intentos de acceso fallidos sin bloquearlos.
- La función de autocompletar del navegador recuerda la respuesta del usuario al recordatorio de la contraseña.
- Vulnerabilidad de redirección abierta, que puede permitir a un atacante redirigir usuarios a un sitio diferente con algunos nombres de dominio especialmente construidos.
- Vulnerabilidad de Java Deserialization en los componentes TunnelServlet y Spring-Remoting services.
- XSS (*Cross-Site Scripting*) y problemas con permisos en la versión 6.2.5.

Las vulnerabilidades más críticas que afectan a la versión 7 son las siguientes:

- Todos los usuarios son administradores (Powe User) por defecto, con lo que el usuario puede crear páginas maliciosas u ofensivas.
- Los tokens CSRF se mantienen en la base de datos, lo que puede facilitar a un atacante el lanzamiento de ataques CSRF.
- Vulnerabilidad de redirección abierta en la autenticación mediante Facebook, lo que podría permitir a un atacante redirigir a otro sitio al usuario.
- Recursos WAB restringidos accesibles
- XSS (*Cross-Site Scripting*) y problemas con permisos en la versión 7.0.0.

Se han observado exploits funcionales publicados en Internet, que permiten a cualquier atacante explotar fácilmente estas vulnerabilidades.

Impacto

En el caso de Drupal, un atacante podría obtener información sensible. Además, en caso de tratarse de un sitio web que cuenta con un formulario de registro personalizado, el atacante podría obtener el control total del servidor que aloja la aplicación.

En el caso de Liferay, un atacante que explotara exitosamente una o varias vulnerabilidades mencionadas, podría obtener el control total del servidor que aloja la aplicación de Liferay vulnerable.

Solución

Tanto Drupal como Liferay han publicado actualizaciones corrigen las vulnerabilidades. Se recomienda actualizar los sitios afectados de inmediato.

En el caso de Drupal, puede descargar la última versión de los siguientes enlaces:

- Si utiliza la rama Drupal 7.x, actualice a la versión 7.44: Drupal core 7.44

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

- Si utiliza la rama Drupal 8.x, actualice a la versión 8.13: Drupal core 8.1.3

Para instrucciones de actualización específicas de acuerdo a su rama, puede revisar el siguiente artículo: https://www.drupal.org/upgrade

En el caso de Liferay, la solución dependerá de la versión:

- Para la versión 6.2: Existen dos parches (aquí y aquí) de los que sólo se debe aplicar uno de ellos, indistintamente.
- Para la versión 7.0: se debe actualizar a Liferay Portal 7.0 CE GA2 (7.0.1)

Para instrucciones de actualización específicas, puede revisar los siguientes artículos:

https://dev.liferay.com/discover/deployment/-/knowledge_base/6-2/patching-liferay

https://dev.liferay.com/discover/deployment/-/knowledge_base/7-0/upgrading-to-liferay-7

Información adicional:

https://dev.liferay.com/web/community-security-team/known-vulnerabilities

https://www.drupal.org/SA-CORE-2016-002

https://www.incibe.es/securityAdvice/CERT/Alerta_Temprana/Avisos_seguridad_tecnicos/multiples_vulnerabilidades_liferay_20160617

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