https://info.nodo50.org/Grave-fallo-de-seguridad-en-SPIP.html

Grave fallo de seguridad en SPIP, urge actualizar

- Nodo50 - Noticias Técnicas -

Fecha de publicación en línea: SÃ¡bado 8 de agosto de 2009

Se ha descubierto un fallo que permite que un atacante remoto tome el control de una instalación de SPIP, y en determinadas circunstancias también del servidor que lo aloja. Afecta a las versiones anteriores a la 2.0.9 y 1.9.2i

Es por tanto muy importante actualizar a las versiones que solucionan el fallo, la 2.0.9 o la 1.9.2i para quien siga usando la rama 1.9.x.

Se sabe que el fallo ya ha sido explotado con el fin de incluir malware en un sitio SPIP.

El anuncio oficial se puede leer en el sitio SPIP-contrib en francés o en inglés.

SPIP es uno de los gestores de contenido mas utilizados por las organizaciones que alojamos en Nodo50. Si tenéis problemas con la actualización recordad que hacemos copias de seguridad diarias de todo, por si necesitáis recurrir a ellas. Y lo mismo si vuestro sitio resultara atacado antes de actualizarlo.

Si no podéis actualizar inmediatamente hay un truco que podéis utilizar para restringir el acceso a la administración de SPIP por IP y limitar las posibilidades de éxito de un atacante. Consiste en crear un archivo llamado .htaccess dentro de la carpeta /ecrire/ de vuestro sitio SPIP con el siguiente contenido:

```
Allow from a.b.c.d
 Deny from All
```

Sustituyendo a.b.c.d por la dirección IP desde donde accedáis a la administración del SPIP. Para autorizar varias IP podéis añadir mas líneas *Allow* (una para cada IP) dejando siempre al final la línea *Deny*. Para saber vuestra dirección IP podéis visitar páginas como esta. Naturalmente si vuestra IP es dinámica deberéis actualizar el fichero .htaccess cada vez que os cambie la IP.