

Herramientas gratuitas para proteger a los usuarios del exploit de IIS

Desde Shavlik Technologies, suministrador de gestión de parches y seguridad, sugieren un par de herramientas gratuitas de Microsoft para ayudar a los usuarios a protegerse contra el ataque de día cero en Internet Information Server.

Eric Schultze, CTO de Shavlik, afirma que IIS Lockdown y URLScan, ambas ofrecidas de forma gratuita por Microsoft, proporcionarán protección a los usuarios hasta que Microsoft decida si lanza un parche formal. URLScan v3.1 es un filtro ISAPI que lee la configuración de un archivo Urlscan.ini y evita que ciertos tipos de peticiones http sean ejecutadas por IIS, según la web de Microsoft. La herramienta se instala con versiones IIS 5.1 y posteriores. Respecto a IIS Lockdown, puede utilizarse con IIS 5.0. Las versiones 6.0 y 7.0 de IIS ya integran herramientas de configuración de seguridad similares y los usuarios no tienen que ejecutar Lockdown en servidores web bajo estas versiones de IIS. Schultze considera que la brecha de día cero es más seria en IIS 5.0 sobre Windows 2000 porque los servicios WebDAV vulnerables se ejecutan por defecto, mientras que IIS 6.0 sobre Windows Server 2003 no permite WebDAV por defecto. En otro punto, el técnico señala que no está claro el nivel de acceso que un hacker puede obtener a través de este exploit. Entre los factores que pueden influir figura el modo en el que está configurado el servidor web y cómo se ha aplicado la seguridad del sistema de archivos a los datos del servidor. "Si el atacante es incapaz de escribir cualquier archivo en el servidor web, es aún menos probable que pueda subir o ejecutar código malicioso en el servidor u obtener niveles de acceso adicionales", asegura este portavoz de Shavlik. Lo que no ha dicho, sin embargo, es que la brecha puede permitir a los atacantes leer páginas de código en el servidor web, las cuales pueden incluir los nombres de usuario y password para aplicaciones o bases de datos controladas por el servidor Web. Schultze recomienda a aquellos que tengan IIS 5.0 o 6.0 que utilicen las herramientas IIS Lockdown y URLScan. Ambas desactivan WebDAV y, en su opinión, protegerán los sistemas de esta última vulnerabilidad.

Autor: CSO

Fuente: <http://www.csospain.es/Herramientas-gratuitas-para-proteger-a-los-usuarios-del-expl/seccion-alertas/noticia-80792>