

Actualización de la vulnerabilidad de Outpost 4.0

En los foros en línea y en diversos medios, existe un gran debate en relación a la capacidad de los cortafuegos, para prevenir el impacto de los códigos maliciosos “en estado salvaje” en la seguridad o la estabilidad del sistema.

El 15 de enero de 2007, David Matoušek presentó los [detalles de un código malicioso](#) que desactiva la autoprotección de Outpost Firewall Pro.

Dos días después, Virus Bulletin publicó un [informe sobre dicho ataque](#), que se aprovecha de una vulnerabilidad de la aplicación.

Agnitum ya conoce la existencia de este problema, y está trabajando en su corrección, que estará disponible para los usuarios a la brevedad. Importante: ha sido corregido en la versión 4.0.1007.

Sin embargo, hay algunos comentarios más para agregar a esta historia.

[Matousec.com](#), el sitio que anunció la vulnerabilidad, fue fundado por David Matoušek en marzo de 2006, y está formado por “un pequeño grupo de jóvenes, en su mayoría estudiantes universitarios, interesados por Internet, la seguridad, y otros temas relacionados con la informática”.

Desafortunadamente, si bien el grupo tiene ciertos conocimientos sobre las cuestiones técnicas relativas a la seguridad de la información, pareciera que no han comprendido los principios éticos básicos de este negocio.

Después de probar Outpost Firewall Pro 4.0, el señor Matoušek se puso en contacto con Agnitum, y sugirió que le [pagáramos por el informe sobre las vulnerabilidades](#) que había descubierto en Outpost Firewall.

Esta actitud nos pareció semejante a una extorsión, y por eso nos negamos a pagar.

En la comunidad de la seguridad informática, existe un principio generalmente aceptado, que establece que, cuando alguien descubre una vulnerabilidad en una aplicación, tiene que comunicarse con el desarrollador del programa, y brindarle gratuitamente toda la información necesaria para que pueda identificar y reparar dicho inconveniente.

Por lo tanto, nos tomó por sorpresa que el señor Matoušek haya decidido publicar por su cuenta los detalles de la vulnerabilidad de Outpost, sin entregarnos los recursos necesarios para encarar el problema directamente y proteger a nuestros clientes.

Todo esto parecería contradecir directamente las afirmaciones del grupo, que sostiene que su objetivo es mejorar la seguridad de los usuarios finales.

Además, es un claro alejamiento de las prácticas comunes de esta industria, como las mencionadas en:

- Rain Forest Puppy,
"Full Disclosure Policy (RFPolicy) v2.0"
- CERT/CC Vulnerability Disclosure Policy
- Organization for Internet Safety,
"Guidelines for Security Vulnerability Reporting and Response, Version 2.0"

De modo que, a diferencia de los demás investigadores, Matoušek pareciera estar tratando de obtener cierta promoción personal, publicando los errores, sin informar previamente a los desarrolladores.

En segundo lugar, Matousec evaluó Outpost sólo después de haber modificado el módulo sandbox.sys de la aplicación ([BTP00003P004AO.zip](#)).

Esto es una clara violación al Contrato de licencia del usuario final (EULA, *End-User-License-Agreement*) y los tratados internacionales de derechos de autor.

En cuanto a la vulnerabilidad en sí, reconocemos que podría convertirse en un riesgo si el usuario ha iniciado sesión con privilegios de administrador, y ejecuta una aplicación desconocida que en realidad es un código malicioso.

Pero, en este caso, el usuario sería igualmente vulnerable, sin importar qué programas de seguridad esté utilizando, pues los intrusos pueden usar este tipo de código para realizar casi todo tipo de actividad maliciosa en el ordenador de su víctima.

En todo caso, me gustaría volver a enfatizar que nosotros tomamos la seguridad de nuestros usuarios finales con extrema seriedad, y un parche que soluciona este inconveniente será lanzado en las próximas semanas.

Mikhail Zakhryapin

Presidente y Director ejecutivo de Agnitum Ltd.

23-Noviembre-2006