BOLETÍN DE ALERTA

Boletín Nro.: 2022-12

Fecha de publicación: 24/2/2022

Tema: Vulnerabilidad de ejecución remota de código (RCE) en *pfSense*.

Software afectado:

- *pfSense* versiones anteriores a 2.5.3.

Descripción:

PfSense ha publicado una actualización de seguridad para una vulnerabilidad crítica, que permitiría a un atacante realizar ejecución remota de código (RCE) en el equipo de la víctima.

La vulnerabilidad fue identificada como CVE-2021-41282, de severidad crítica, sin puntuación asignada. Esta se debe a una incorrecta validación de datos de entrada de la utilidad *sed* (editor de secuencias) de *pfSense*, que permitiría a un atacante realizar ejecución remota de código (RCE) en el equipo de la víctima.

PfSense permite a usuarios autenticados obtener información sobre las rutas establecidas en el firewall. Dicha información se obtiene ejecutando la utilidad ***netstat***, su salida se analiza a través de la utilidad ***sed*** (editor de secuencias). Si bien los patrones de prevención comunes para inyecciones de comandos están activos, aún es posible inyectar código específico de *sed*, así como escribir un archivo arbitrario en una ubicación arbitraria con el fin de realizar ejecución remota de código (RCE).

Impacto:

La explotación de esta vulnerabilidad permitiría a un atacante realizar ejecución remota de código (RCE) en equipo de la víctima.

Detección:

Para comprobar si su aplicación es vulnerable debe verificar si la versión de *pfSense*, corresponde a las siguientes:

- *pfSense* versiones anteriores a 2.5.3.

Solución:

Recomendamos instalar las actualizaciones de seguridad correspondientes provistas por *pfSense*, como se indica en la siguiente guía.

- *PfSense 2.6.0* https://www.pfsense.org/download/

Información adicional:

- https://www.netgate.com/blog/pfsense-plus-software-version-22.01-and-ce-2.6.0-are-now-available
- https://www.shielder.it/advisories/pfsense-remote-command-execution/
- https://twitter.com/ptracesecurity/status/1496658763826315268?t=OrYP5801OKjwCC-ekNdJ4g&s=09