Actualizaciones de Seguridad para FortiOS, FortiProxy y FortiClient

El fabricante de los productos Fortinet ha reportado sobre vulnerabilidades críticas en distintos productos de seguridad, incluyendo FortiProxy, FortiOS y FortiClient. Estas vulnerabilidades podrían permitir a atacantes tomar control de sus sistemas y robar información sensible.

Productos o items afectados

- Fortinet FortiProxy versiones 7.4.0, 7.2.0 - 7.2.6, 7.0.0 - 7.0.12, 2.0.0 - 2.0.13, 1.2.0 - 1.2.13, 1.1.0 - 1.1.6, 1.0.0 - 1.0.7.
- Fortinet FortiOS versiones 7.4.0 - 7.4.1, 7.2.0 - 7.2.6, 7.0.0 - 7.0.12, 6.4.0 - 6.4.14, 6.2.0 - 6.2.15, 6.0.0 - 6.0.17.
- Fortinet FortiClientLinux versiones 7.2.0, 7.0.6 - 7.0.10 y 7.0.3 - 7.0.4.
- Instalador de Fortinet FortiClientMac

Impacto de la vulnerabilidad

CVE-2023-45590: Vulnerabilidad donde una incorrecta gestión de la generación de código ('inyección de código') en Fortinet FortiClientLinux permitiría a un actor malicioso ejecutar código o comandos no autorizados al engañar a un usuario de FortiClientLinux para que visite un sitio web malicioso. Se ha asignado una puntuación en CVSSv3 de 9.4 con una severidad alta.

CVE-2023-45588 y **CVE-2024-31492** ambas vulnerabilidades según el fabricante del producto Fortinet, con un comportamiento parecido se ha asignado ambas vulnerabilidades a la descripción, donde una falla en el control externo de nombre de archivo o ruta en el instalador de FortiClientMac puede permitir que un actor malicioso posicionado de manera local en el equipo afectado, ejecute código o comandos arbitrarios mediante la escritura de un archivo de configuración malicioso en /tmp antes de iniciar el proceso de instalación. Se ha asignado una puntuación de 8.2 en CVSSv3 con una severidad alta.

CVE-2023-41677: Vulnerabilidad donde las credenciales insuficientemente protegidas en Fortinet FortiProxy, Fortinet FortiOS podrían permitir a un actor malicioso ejecutar código arbitrario, comandos no autorizados a través de un ataque de ingeniería social dirigido. Se ha asignado una puntuación de 7.5 en CVSSv3 con una severidad alta.

Recomendaciones

El fabricante del producto ha liberado parches de seguridad para sus productos, se recomienda, actualizar a la última versión disponible según el producto afectado.

Referencias

- https://www.fortiguard.com/psirt/FG-IR-23-493
- https://www.fortiguard.com/psirt/FG-IR-23-087
- https://www.fortiguard.com/psirt/FG-IR-23-345