Fortinet ha revelado que actores maliciosos han encontrado una forma de mantener acceso de solo lectura a dispositivos FortiGate vulnerables incluso después de que se haya parcheado el vector de acceso inicial utilizado para comprometer los dispositivos.

Se cree que los atacantes aprovecharon vulnerabilidades conocidas y ya corregidas, incluidas, pero no limitadas a, CVE-2022-42475, CVE-2023-27997 y CVE-2024-21762.

> *«Un actor de amenazas utilizó una vulnerabilidad conocida para implementar acceso de solo lectura a dispositivos FortiGate vulnerables. Esto se logró mediante la creación de un enlace simbólico que conecta el sistema de archivos del usuario con el sistema de archivos raíz en una carpeta utilizada para servir archivos de idioma del SSL-VPN»,* indicó la empresa de seguridad de red en un comunicado publicado el jueves.

Fortinet dijo que las modificaciones ocurrieron en el sistema de archivos del usuario y lograron evadir la detección, lo que provocó que el enlace simbólico (también conocido como symlink) permaneciera incluso después de que se solucionaron las vulnerabilidades responsables del acceso inicial.

Esto, a su vez, permitió que los actores de amenazas mantuvieran acceso de solo lectura a los archivos del sistema de archivos del dispositivo, incluidas las configuraciones. Sin embargo, los clientes que nunca habilitaron SSL-VPN no se ven afectados por este problema.

No está claro quién está detrás de esta actividad, pero Fortinet indicó que su investigación reveló que no estaba dirigida a ninguna región o industria específica. También señaló que notificó directamente a los clientes que se vieron afectados por el problema.

Como medidas adicionales para prevenir que este tipo de incidentes vuelva a ocurrir, se han implementado una serie de actualizaciones de software para FortiOS:

- FortiOS 7.4, 7.2, 7.0, 6.4: El enlace simbólico fue marcado como malicioso para que

sea eliminado automáticamente por el motor antivirus.
- FortiOS 7.6.2, 7.4.7, 7.2.11, 7.0.17 y 6.4.16: El enlace simbólico fue eliminado y la interfaz de usuario de SSL-VPN fue modificada para evitar la entrega de enlaces simbólicos maliciosos.

Se recomienda a los clientes actualizar sus instancias a las versiones FortiOS 7.6.2, 7.4.7, 7.2.11, 7.0.17 o 6.4.16, revisar las configuraciones de los dispositivos, tratar todas las configuraciones como potencialmente comprometidas y realizar los pasos de recuperación apropiados.

La Agencia de Ciberseguridad y Seguridad de Infraestructura de EE. UU. (CISA) emitió su propio aviso, instando a los usuarios a restablecer las credenciales expuestas y considerar deshabilitar la funcionalidad de SSL-VPN hasta que se puedan aplicar los parches. El Equipo de Respuesta ante Emergencias Informáticas de Francia (CERT-FR), en un boletín similar, dijo estar al tanto de compromisos que se remontan hasta principios de 2023.

En una declaración, el CEO de watchTowr, Benjamin Harris, dijo que el incidente es preocupante por dos razones importantes:

> *"Primero, la explotación en estado salvaje está ocurriendo significativamente más rápido de lo que las organizaciones pueden aplicar parches. Más importante aún, los atacantes son consciente y profundamente conscientes de este hecho",* dijo Harris.
>
> *"Segundo, y más aterrador, hemos visto en numerosas ocasiones a los atacantes desplegar capacidades y puertas traseras tras una explotación rápida, diseñadas para sobrevivir a los procesos de parcheo, actualización y restablecimiento de fábrica en los que las organizaciones han llegado a confiar para mitigar estas situaciones y mantener la persistencia y el acceso a las organizaciones comprometidas".*