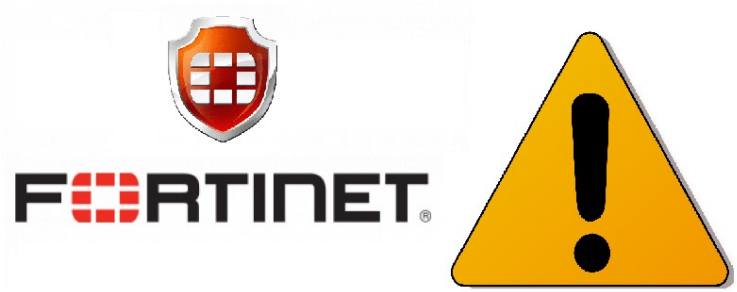
CREDENCIALES DE VPN FORTINET EXPUESTAS EN INTERNET (13/SEPTIEMBRE/2021)



Ciber atacantes habrían expuesto credenciales de VPN Fortinet, poniendo en riesgo la confidencialidad de la información gestionada por estos dispositivos.

Una vulnerabilidad en el FortiOS SSL VPN web portal de tipo “path traversal” es decir acceso a rutas que contienen archivos sensibles de configuración y bases de datos, ha sido explotada por ciber atacantes a través de diversos mecanismos, mismos que han sido gestionados por el desarrollador ante la detección de cada una de las campanas de explotación.

En consideración al alto riesgo contra la confidencialidad, integridad y disponibilidad de los activos de información administrados por la herramienta Microsoft Exchange, el EcuCERT recomienda a su comunidad objetivo, tomar en consideración las siguientes recomendaciones:

1. Actualizar la versión del software que gestiona las VPNs,

2. Actualizar las credenciales de todos los usuarios de VPNs.

3. En caso de ser factible implementar procesos de múltiple factor de autenticación a fin de mitigar el posible comprometimiento de credenciales filtradas.

4. Notificar a los usuarios las razones del porque se realiza una actualización de las credenciales de acceso y alertar respecto de posibles correos electrónicos ilegítimos señalando la necesidad de actualizar o cambiar las cred3enciales de acceso de VPN Fortinent.

Referencias

FORTINET. (2021). Malicious Actor Discloses FortiGate SSL-VPN Credentials. Disponible en https://www.fortinet.com/blog/psirt-blogs/malicious-actor-discloses-fortigate-ssl-vpn-credentials

FORTIGUARD LABS. (2019). FortiOS system file leak through SSL VPN. Disponible en https://www.fortiguard.com/psirt/FG-IR-18-384

CVE. (2018). CVE-2018-13379. Disponible en http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-13379