09.09.2021
DIVISIÓN DE REDES Y SEGURIDAD INFORMÁTICA
CSIRT DE GOBIERNO

Alerta ante filtración de claves de VPN Fortinet (Septiembre 2021)

Ante la divulgación por parte de una banda de cibercriminales de casi 500 mil credenciales de autenticación de distintos productos VPN provistos por Fortinet[1], el CSIRT de Gobierno llama a los encargados de ciberseguridad que administren VPN de Fortinet a:

1. Forzar el cambio de contraseñas de todos sus usuarios VPN cuanto antes.

2. Cambiar las contraseñas de los usuarios administradores de su equipamiento VPN Fortinet.

3. Corroborar que hayan actualizado sus sistemas con todos los parches provistos por Fortinet, especialmente en este caso para las vulnerabilidades que habrían hecho posible el robo de las credenciales en primer lugar.

   Estas son vulnerabilidades que ya han sido comunicadas por el proveedor:

   a. CVE-2020-12812 de 2020: https://www.csirt.gob.cl/vulnerabilidades/9vsa20-00272-01/.

   b. CVE-2018-13379 de 2019: https://www.csirt.gob.cl/vulnerabilidades/9vsa-00032-001-csirt-comparte-actualizaciones-de-fortninet-para-varios-de-sus-productos/.

   c. CVE-2019-5591 de 2019: https://www.fortiguard.com/psirt/FG-IR-19-037.

4. Evaluar la disposición de su arquitectura para proteger el administrador de las VPN.

5. Revisar y auditar las conexiones a sus sistemas VPN para detectar algún posible mal uso por terceras partes no autorizadas.

6. En caso de detectar conexiones sospechosas, bloquear esas cuentas o cambiar su contraseña (teniendo en cuenta que si no se ha parchado el dispositivo, rápidamente pueden volver a quedar expuestas las nuevas credenciales) e indagar posibles acciones maliciosas dentro de

[1] https://www.bleepingcomputer.com/news/security/hackers-leak-passwords-for-500-000-fortinet-vpn-accounts/.

la red interna, tales como el acceso a datos sensibles, el ingreso de malware/ransomware o la creación de backdoors para accesos futuros.

7. De existir la confirmación de acciones maliciosas se solicita notificar al CSIRT de Gobierno y coordinarse con sus equipos jurídicos para hacer las denuncias pertinentes ante la materialización de un delito informático.

El actor malicioso responsable de la filtración indica a través de los foros de la Darknet conocidos como RAMP y Groove, en los que publicó el leak, que los usuarios y contraseñas son válidos. De ser esto efectivo, esto permite a terceras partes tener acceso a la red interna de las organizaciones afectadas.

El CSIRT de Gobierno han identificado 247 IP de Chile entre las filtradas, y se encuentra en proceso de notificarlas caso a caso y de forma privada, por motivos de seguridad.

.

CSIRT Gobierno de Chile

Firmado digitalmente por CSIRT Gobierno de Chile
Fecha: 2021.09.09 12:55:23 -03'00'