*Nota: Documento catalogado como TLP blanco, es decir, la información puede ser distribuida sin restricciones, sujeta a controles de Copyright.

ACTUALIZACIÓN ALERTA DE SEGURIDAD CIBERNÉTICA
VULNERABILIDAD CVE-2022-1388 EN BIG-IP DE F5

El CSIRT de Gobierno reitera su llamado a todas las instituciones del Estado y privados del país a estar alertas y tomar las medidas de mitigación necesarias ante la vulnerabilidad crítica conocida bajo el código CVE-2022-1388, la cual fue motivo de una alerta del CSIRT de Gobierno publicada el 5 de mayo en la siguiente dirección de nuestro sitio web oficial: https://www.csirt.gob.cl/noticias/alerta-de-seguridad-cibernetica-big-ip/.

Es de crucial importancia que toda institución y empresa aplique de inmediato los parches hechos disponibles por F5 o, de no ser aún posible, bloquear todo el acceso a la interfaz REST de iControl en el sistema BIG-IP, como recomienda F5. Los detalles de mitigación se pueden encontrar en: https://support.f5.com/csp/article/K23605346.

Se ha podido constatar que ya existen intentos de explotación de esta vulnerabilidad en la Red de Conectividad del Estado. Es por esto que el CSIRT de Gobierno, en conjunto con la Red de Conectividad del Estado, hemos realizado bloqueos preventivos y automatizados a través de nuestros equipos perimetrales.

IoC: IP que han sido visualizadas intentando explotar la vulnerabilidad CVE-2022-1388 y que consiguientemente han sido bloqueadas.

IP	ASN
173.255.238.253	Linode, LLC
94.177.118.129	ASN-GIGENET
80.94.92.38	Pptechnology Limited
20.187.67.224	MICROSOFT-CORP-MSN-AS-BLOCK
164.92.146.169	DIGITALOCEAN-ASN
125.160.201.91	PT Telekomunikasi Indonesia
45.61.139.143	BLNWX
103.165.85.137	Nathosts Limited
103.165.85.136	Nathosts Limited
121.237.233.221	Chinanet
218.205.242.246	China Mobile Communications Group Co., Ltd.
121.237.233.221	Chinanet

Color	¿Cuándo se debe usar?	¿Cómo se puede compartir?
TLP: ROJO - No es para divulgación, restringida solo a los participantes.	Se debe utilizar "TLP: ROJO "cuando la información está limitada a personas concretas, y podría tener impacto en la privacidad, reputación u operaciones si es mal utilizada.	Los receptores no deben compartir información designada como "TLP: ROJO "con ningún tercero fuera del ámbito donde fue expuesta originalmente. En la mayoría de las circunstancias, TLP:RED debe intercambiarse verbalmente o en persona.
TLP: ÁMBAR - Divulgación limitada, restringida a las organizaciones de participantes.	Se debe utilizar "TLP: AMBAR" cuando la información requiere ser distribuida de forma limitada, pero supone un riesgo para la privacidad, reputación u operaciones si es compartida fuera de la organización.	Los receptores pueden compartir información indicada como "TLP: AMBAR" únicamente con miembros de su propia organización que necesitan conocerla, y con clientes, proveedores o asociados que necesitan conocerla para protegerse a sí mismos o evitar daños. El emisor puede especificar restricciones adicionales para compartir esta información.
TLP: VERDE - Divulgación limitada, restringida a la comunidad.	Se debe utilizar "TLP: VERDE" cuando la información es útil para todas las organizaciones que participan, así como con terceros de la comunidad o del sector	Los receptores pueden compartir la información indicada como "TLP: VERDE" con organizaciones afiliadas o miembros del mismo sector, pero nunca a través de canales públicos.
TLP: BLANCO - La divulgación no está limitada.	Se debe utilizar "TLP: BLANCO" cuando la información no supone ningún riesgo de mal uso, dentro de las reglas y procedimientos establecidos para su difusión pública.	La información "TLP: BLANCO" puede ser distribuida sin restricciones, sujeta a controles de Copyright.