Alerta de Seguridad Cibernética

Alerta de seguridad cibernética	9VSA22-00629-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Crítico
TLP	Blanco
Fecha de lanzamiento original	5 de mayo de 2022
Última revisión	5 de mayo de 2022

NOTIFICACIÓN

La información consignada en el presente informe es producto del análisis de múltiples fuentes, de terceras partes, del propio fabricante e investigación propia del CSIRT de Gobierno. La información contenida en los informes o comunicados está afecta a actualizaciones.

Resumen

El Equipo de Respuesta ante Incidentes de Seguridad Informática del Gobierno de Chile, CSIRT de Gobierno, comparte información sobre una nueva vulnerabilidad crítica conocida para el producto BIG-IP de F5.

Este informe incluye las medidas de mitigación, consistentes en instalar la última actualización de los productos afectados.

Vulnerabilidades

CVE-2022-1388

Impacto

Vulnerabilidades críticas

CVE-2022-1388: Esta vulnerabilidad surge de un error en la interfaz REST del iControl framework, usado para comunicarse entre aparatos F5 y los usuarios. La vulnerabilidad puede permitir a un atacante no autenticado con acceso de red a un sistema BIG-IP a través de un puerto de administración o un self-IP address (direcciones IP en un sistema BIG-IP, usadas para asociarse con VLAN), la ejecución arbitraria de comandos, crear o borrar archivos, o deshabilitar servicios.

Productos afectados

BIG-IP, versiones:
16.1.0 a 16.1.2
15.1.0 a 15.1.5
14.1.0 a 14.1.4
13.1.0 a 13.1.4
12.1.0 a 12.1.6 (no serán parchados)

11.6.1 a 11.6.5 (no serán parchados)

Mitigación

Instalar las respectivas actualizaciones entregadas por el proveedor.

Enlaces

https://support.f5.com/csp/article/K23605346
https://www.cisa.gov/uscert/ncas/current-activity/2022/05/04/f5-releases-security-advisories-addressing-multiple
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-1388

CSIRT Gobierno de Chile

Firmado digitalmente por CSIRT Gobierno de Chile
Fecha: 2022.05.05 11:16:01 -04'00'