Alerta de seguridad cibernética	9VSA22-00746-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	17 de noviembre de 2022
Última revisión	17 de noviembre 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, CSIRT de Gobierno, comparte información entregada por F5 sobre vulnerabilidades en algunos de sus productos.

Vulnerabilidades

CVE-2022-41622 y CVE-2022-41800

Impacto

Vulnerabilidades de mayor riesgo (riesgo alto)

CVE-2022-41622 (CVSS: 8.8): Vulnerabilidad CSRF a través de iControl SOAP, que puede llevar a la ejecución remota de código.

CVE-2022-41800 (CVSS: 8.7): Vulnerabilidad de iControl REST que podría permitir a un usuario autenticado con rol de Administrador evadir las restricciones del modo Appliance.

Productos afectados

BIG-IP 13.x, 14.x, 15.x, 16.x, y 17.x
BIG-IQ Centralized Management versiones 7.x y 8.x.

Mitigación

Instalar las respectivas actualizaciones entregadas por el proveedor.

Enlaces

https://support.f5.com/csp/article/K97843387
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-41800
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-41622

CSIRT Gobierno de Chile

Firmado digitalmente por CSIRT Gobierno de Chile
Fecha: 2022.11.17 11:26:47 -03'00'

CONTACTO Y REDES SOCIALES DEL CSIRT DE GOBIERNO

https://www.csirt.gob.cl
Teléfonos: 1510 | + (562) 24863850 | Correo: soc-csirt@interior.gob.cl
@csirtgob
https://www.linkedin.com/company/csirt-gob