Alerta de Seguridad Cibernética

Alerta de seguridad cibernética	9VSA22-00605-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Crítico
TLP	Blanco
Fecha de lanzamiento original	4 de abril de 2022
Última revisión	4 de abril 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 vulnerabilidad crítica en Spring Framework. La vulnerabilidad se encuentra siendo explotada y ha sido apodada como “Spring4Shell”.

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

Vulnerabilidad

CVE-2022-22965

Impacto

Esta vulnerabilidad crítica permite a un atacante remoto ejecutar código arbitrario en el sistema objetivo. La vulnerabilidad existe debido a una inapropiada validación de inputs. La explotación exitosa de esta vulnerabilidad puede resultar en un compromiso total de un sistema vulnerable.

Productos afectados

Pivotal Spring Framework: versiones 5.0.0 - 6.0.0-M3.

Mitigación

Instalar las respectivas actualizaciones entregadas por el proveedor.

Enlaces

https://spring.io/blog/2022/03/31/spring-framework-rce-early-announcement
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-22965

CSIRT Gobierno de Chile

Firmado digitalmente por CSIRT Gobierno de Chile
Fecha: 2022.04.04 11:57:36 -04'00'