06.04.2022
DIVISIÓN DE REDES Y SEGURIDAD INFORMÁTICA
CSIRT DE GOBIERNO

Información sobre proveedores afectados por "Spring4Shell"

A fines de marzo se dio conocer la existencia de una vulnerabilidad crítica que afecta a Spring, un framework de Java ampliamente utilizado (algunas estimaciones señalan que es la más popular del mundo). La vulnerabilidad, apodada **"Spring4Shell"** fue identificada como **CVE-2022-22965** y publicada en su momento por el CSIRT de Gobierno. Sus detalles pueden verse aquí: https://www.csirt.gob.cl/vulnerabilidades/9vsa22-00605-01/.

Varias empresas que usan Spring para desarrollar algunos de sus productos han identificado aquellos que estarían afectados por la vulnerabilidad, y entregado parches para corregirla. Algunos de las principales son **VMware, Cisco, Red Hat, SolarWinds y SAP,** cuyos detalles y enlaces respectivos se detallan en el presente documento.

Es muy importante que las organizaciones identifiquen si sus sistemas cuentan con programas vulnerables a esta amenaza, la que se teme que pueda ser ampliamente por ciberdelincuentes. Tanto es así que ya la empresa de ciberseguridad Check Point asegura que alrededor de un sexto de las empresas con software vulnerable ya han sido atacadas[1].

Proveedor: VMware

Productos afectados

VMware Tanzu Application Service for VMs
VMware Tanzu Operations Manager
VMware Tanzu Kubernetes Grid Integrated Edition (TKGI)

Más información:
https://www.vmware.com/security/advisories/VMSA-2022-0010.html
https://www.csirt.gob.cl/vulnerabilidades/9vsa22-00608-01/

Proveedor: Cisco

Productos confirmados por Cisco como afectados hasta el momento de la redacción de este documento:

Cisco Crosswork Optimization Engine
Cisco Crosswork Zero Touch Provisioning (ZTP)
Cisco Edge Intelligence

[1] https://www.bleepingcomputer.com/news/security/springshell-attacks-target-about-one-in-six-vulnerable-orgs/

Más información (en estos enlaces de Cisco, la empresa actualizará con más productos confirmados o descartados como afectados):
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-java-spring-rce-Zx9GUc67
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-java-spring-scf-rce-DQrHhJxH
https://www.csirt.gob.cl/vulnerabilidades/9vsa22-00609-01/

Proveedor: Red Hat

Productos afectados:
Red Hat Descision Manager 7
Red Hat JBoss A-MQ 6
Red Hat JBoss Fuse 6
Red Hat JBoss Fuse 7
Red Hat Process Automation 7
Red Hat JBoss A-MQ 7
Red Hat Virtualization 4

Más información:
https://access.redhat.com/security/cve/CVE-2022-22965
https://access.redhat.com/security/vulnerabilities/RHSB-2022-003

Proveedor: SolarWinds

Productos en investigación (no confirmados ni descartados como afectados):
Security Event Manager (SEM)
Database Performance Analyzer (DPA)
Web Help Desk (WHD)

Más información:
https://www.solarwinds.com/fr/trust-center/security-advisories/spring4shell

Proveedor: SAP

Productos afectados:
SAP NetWeaver Application Server for Java todas las versiones.

Más información:
https://userapps.support.sap.com/sap/support/knowledge/en/3171058

CSIRT Gobierno de Chile
Firmado digitalmente por CSIRT Gobierno de Chile
Fecha: 2022.04.06 10:07:25 -04'00'