Alerta de Seguridad Cibernética

Alerta de seguridad cibernética	9VSA22-00657-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Crítico
TLP	Blanco
Fecha de lanzamiento original	15 de junio de 2022
Última revisión	15 de junio 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 compartida por Cisco sobre nuevas vulnerabilidades que afectan a algunos de sus productos.

Vulnerabilidades

CVE-2021-1579
CVE-2022-22965
CVE-2022-20742
CVE-2022-20742
CVE-2022-20715
CVE-2022-20759
CVE-2022-20745
CVE-2022-20737
CVE-2022-20760
CVE-2022-20774
CVE-2022-20821
CVE-2022-20806
CVE-2022-20807
CVE-2022-20809

Impacto

Vulnerabilidades de riesgo crítico:

CVE-2022-22965: Vulnerabilidad en el Spring Framework, que afecta a las aplicaciones Spring MVC y Spring WebFlux que corren en JDK 9+.

Productos afectados

Cisco CX Cloud Agent Software
Cisco Automated Subsea Tuning
Cisco Crosswork Network Controller
Cisco Crosswork Optimization Engine
Cisco Crosswork Zero Touch Provisioning (ZTP)

Cisco DNA Center
Cisco Evolved Programmable Network Manager
Cisco Managed Services Accelerator (MSX)
Cisco Optical Network Planner
Cisco WAN Automation Engine (WAE) Live
Cisco WAN Automation Engine (WAE)
Data Center Network Manager (DCNM)
Nexus Dashboard Fabric Controller (NDFC)
Cisco Optical Network Controller
Cisco Software-Defined AVC (SD-AVC)
Cisco Enterprise Chat and Email
Cisco Meeting Server
Cisco APIC
Cisco Cloud APIC Software
Cisco ASA Software
Cisco FTD Software
Cisco IP Phone 6800 Series con Multiplatform Firmware
Cisco IP Phone 7800 Series con Multiplatform Firmware
Cisco IP Phone 8800 Series con Multiplatform Firmware
Cisco Expressway Series
Cisco TelePresence VCS

Mitigación

Instalar las respectivas actualizaciones entregadas por el proveedor.

Enlaces

https://tools.cisco.com/security/center/publicationListing.x
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-1579
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-22965
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-20742
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-20742
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-20715
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-20759
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-20745
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-20737
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-20760
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-20774
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-20821
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-20806
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-20807
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-20809

CSIRT Gobierno de Chile
Firmado digitalmente por CSIRT Gobierno de Chile
Fecha: 2022.06.15 11:07:40 -04'00'