Alerta de Seguridad Cibernética

Alerta de seguridad cibernética	9VSA22-00678-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Crítico
TLP	Blanco
Fecha de lanzamiento original	21 de julio de 2022
Última revisión	21 de julio 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 sobre nuevas vulnerabilidades dadas a conocer por Cisco.

Vulnerabilidades

CVE-2022-20857
CVE-2022-20858
CVE-2022-20861
CVE-2022-20860
CVE-2022-20873
CVE-2022-20874
CVE-2022-20875
CVE-2022-20876
CVE-2022-20877
CVE-2022-20878
CVE-2022-20879
CVE-2022-20880
CVE-2022-20881
CVE-2022-20882
CVE-2022-20883
CVE-2022-20884
CVE-2022-20885
CVE-2022-20886
CVE-2022-20887
CVE-2022-20888
CVE-2022-20889
CVE-2022-20890
CVE-2022-20891
CVE-2022-20892
CVE-2022-20893
CVE-2022-20894
CVE-2022-20895
CVE-2022-20896
CVE-2022-20897
CVE-2022-20898
CVE-2022-20899
CVE-2022-20900
CVE-2022-20901
CVE-2022-20902
CVE-2022-20903
CVE-2022-20904
CVE-2022-20910
CVE-2022-20911
CVE-2022-20912
CVE-2022-20906
CVE-2022-20907
CVE-2022-20908
CVE-2022-20909
CVE-2022-20913
CVE-2022-20916
CVE-2022-20733

Impacto

Vulnerabilidades de riesgo crítico

CVE-2022-20857: Vulnerabilidad de ejecución arbitraria de comandos en Cisco Nexus Dashboard. Un atacante remoto no autenticado puede acceder a una API specifica que esté corriendo en la red de datos y ejecutar comandos arbitrarios en un equipo afectado.

CVE-2022-20858: Vulnerabilidad de escritura y lectura en Cisco Nexus Dashboard Container Image, que puede permitir a un atacante remoto no autenticado acceder a un servicio que esté corriendo en las redes de administración y datos del aparato afectado.

CVE-2022-20861: Vulnerabilidad tipo cross-site request forgery (CSFR) en Cisco Nexus Dashboard. Permite que un atacante remoto no autenticado lleve a cabo un ataque de tipo cross-site request forgery en el equipo afectado.

Productos afectados

Cisco Nexus Dashboard
Cisco Small Business RV110W, RV130, RV130W, and RV215W Routers
Cisco IoT Control Center

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-2022-20857
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-20858
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-20861
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-20860
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-20873
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-20874
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-20875
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-20876
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-20877
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-20878
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-20879
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-20880
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-20881
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-20882
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-20883
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-20884
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-20885
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-20886
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-20887
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-20888
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-20889
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-20890
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-20891
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-20892
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-20893
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-20894
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-20895

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-20896
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-20897
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-20898
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-20899
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-20900
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-20901
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-20902
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-20903
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-20904
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-20910
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-20911
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-20912
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-20906
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-20907
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-20908
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-20909
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-20913
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-20916
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-20733

CSIRT Gobierno de Chile

Firmado digitalmente por CSIRT Gobierno de Chile
Fecha: 2022.07.22 15:23:53 -04'00'