Alerta de seguridad cibernética	9VSA23-00810-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Crítico
TLP	Blanco
Fecha de lanzamiento original	5 de abril de 2023
Última revisión	5 de abril de 2023

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 CSIRT de Gobierno comparte información de vulnerabilidades parchadas por Cisco para varios de sus productos.

Vulnerabilidades

CVE-2022-20812
CVE-2022-20959
CVE-2022-20813
CVE-2023-20064
CVE-2022-20797
CVE-2022-20952
CVE-2023-20113
CVE-2023-20099
CVE-2022-20956
CVE-2022-20964
CVE-2022-20965
CVE-2022-20966
CVE-2022-20967
CVE-2023-20029
CVE-2023-20016
CVE-2023-20027
CVE-2023-20065
CVE-2023-20035
CVE-2023-20072
CVE-2023-20080
CVE-2023-20067
CVE-2023-20055
CVE-2023-20082
CVE-2023-20011
CVE-2023-20113
CVE-2023-20029
CVE-2023-20016
CVE-2023-20027
CVE-2023-20065
CVE-2023-20035
CVE-2023-20072
CVE-2023-20080
CVE-2023-20067
CVE-2023-20055
CVE-2023-20082

Impacto

Vulnerabilidades de riesgo crítico

CVE-2022-20812 y CVE-2022-20813: Vulnerabilidades en la API y la interfaz de administración web de Cisco Expressway Series y Cisco TelePresence Video Communication Server (VCS) que pueden permitir a un atacante remoto sobreescribir archivos arbitrarios o realizar ataques de envenenamiento null byte en un aparato afectado.

Productos afectados

Software Cisco Expressway Series y Cisco TelePresence VCS en configuración por defecto.

Si utilizan software Cisco IOS XR:
ASR 9000 Series Aggregation Services Routers (64-bit) (CSCwd35552)
IOS XR White box (IOSXRWBD) (CSCwd35552)
IOS XRv 9000 Routers (CSCwd35552)
Network Convergence System (NCS) 540 Series Routers (CSCwd35552)
NCS 560 Series Routers (CSCwd35552)
NCS 1001 Series Routers (CSCwd35552)
NCS 1002 Series Routers (CSCwd35552)
NCS 1004 Series Routers (CSCwd35552)
NCS 4000 Series Routers (CSCwc97333)
NCS 5000 Series Routers (CSCwd35552)
NCS 5500 Series Routers (CSCwd35552)
NCS 5700 Series Routers (CSCwd35552)
NCS 6000 Series Routers (CSCwc97332)

Cisco Secure Network Analytics.
Cisco Secure Web Appliance, virtual y hardware.
Cisco Identity Services Engine (ISE).
Cisco APIC.
Cisco Cloud Network Controller.
Cisco SD-WAN vManage Software.

Si usan el Cisco IOS XE Software:
Catalyst 9200 Series Switches
Catalyst 9300 Series Switches

Si usan Cisco FXOS or Cisco UCS Manager Software:
Firepower 4100 Series
Firepower 9300 Security Appliances
UCS 6200 Series Fabric Interconnects
UCS 6300 Series Fabric Interconnects
UCS 6400 Series Fabric Interconnects
UCS 6500 Series Fabric Interconnects

Si usan Cisco IOS XE Software con la función VFR activada:
1000 Series Integrated Services Routers
4000 Series Integrated Services Routers
Catalyst 8000V Edge Software Routers
Catalyst 8200 Series Edge Platforms
Catalyst 8300 Series Edge Platforms
Catalyst 8500L Series Edge Platforms
Cloud Services Router 1000V Series

Productos Cisco corriendo Cisco IOS XE Software releases 17.9.1, 17.9.1a, o 17.9.1w con la tunnel interface configurada.

Aparatos Cisco que se encuentren ejecutando versiones vulnerables de software Cisco IOS o IOS XE y tienen IPv6 y la función servidor o relay DHCPv6 activada.

Los siguientes productos de Cisco si corren una versión vulnerable del software Cisco IOS XE para WLC y tienen la función de perfilamiento de cliente basado en HTTP:
Catalyst 9800 Embedded Wireless Controllers for Catalyst 9300, 9400, and 9500 Series Switches
Catalyst 9800 Series Wireless Controllers
Catalyst 9800-CL Wireless Controllers for Cloud
Embedded Wireless Controllers on Catalyst Access Points

Cisco DNA Center en la configuración por defecto.

Switches Cisco Catalyst 9300 Series si corren software Cisco IOS XE con una versión de Cisco IOS XE ROM Monitor (ROMMON) anterior a las 17.3.7r, 17.6.5r o 17.8.1r.

Cisco SD-WAN vManage Software.

Si corren una versión vulnerable de Cisco IOS XE Software:
Catalyst 9200 Series Switches
Catalyst 9300 Series Switches

Si corren una versión vulnerable de Cisco FXOS or Cisco UCS Manager Software:
Firepower 4100 Series
Firepower 9300 Security Appliances
UCS 6200 Series Fabric Interconnects
UCS 6300 Series Fabric Interconnects
UCS 6400 Series Fabric Interconnects
UCS 6500 Series Fabric Interconnects

Si corren una versión vulnerable de Cisco IOS XE Software con la función VFR activada:
1000 Series Integrated Services Routers
4000 Series Integrated Services Routers
Catalyst 8000V Edge Software Routers
Catalyst 8200 Series Edge Platforms
Catalyst 8300 Series Edge Platforms
Catalyst 8500L Series Edge Platforms
Cloud Services Router 1000V Series

Productos Cisco si corren Cisco IOS XE Software, tienen la función Cisco IOx de hosting configurada y la aplicación está corriendo.

Enlaces

https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-expressway-overwrite-3buqW8LH#vp
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-20812
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-20959

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-20813
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-20064
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-20797
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-20952
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-20113
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-20099
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-20956
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-20964
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-20965
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-20966
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-20967
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-20029
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-20016
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-20027
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-20065
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-20035
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-20072
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-20080
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-20067
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-20055
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-20082
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-20011
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-20113
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-20029
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-20016
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-20027
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-20065
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-20035
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-20072
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-20080
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-20067
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-20055
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-20082

CSIRT Gobierno de Chile

Firmado digitalmente por CSIRT Gobierno de Chile
Fecha: 2023.04.05 17:45:49 -04'00'