Alerta de seguridad cibernética	9VSA21-00487-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	02 de septiembre de 2021
Última revisión	02 de septiembre de 2021

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 equipo CSIRT. 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 vulnerabilidades en productos de Cisco, incluyendo algunas de alto riesgo.

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

Vulnerabilidades

CVE-2019-1727
CVE-2021-1518
CVE-2021-1578
CVE-2021-1579
CVE-2021-1580
CVE-2021-1581
CVE-2021-1582
CVE-2021-1587
CVE-2021-1588
CVE-2021-1590
CVE-2021-1591
CVE-2021-1592
CVE-2021-22156
CVE-2021-34732
CVE-2021-34733
CVE-2021-34746
CVE-2021-34759
CVE-2021-34765

Impactos

Nivel de riesgo crítico:

CVE-2021-34746: Vulnerabilidad de evasión de autenticación en Cisco Enterprise NFV Infrastructure Software.

CVE-2021-22156: Vulnerabilidad de desbordamiento de enteros en software de BlackBerry: QNX SDP 6.5.0SP1 y anteriores, QNX OS for Medical 1.1 y anteriores y QNX OS for Safety 1.0.1 y anteriores.

Nivel de riesgo alto:

CVE-2021-1578: Vulnerabilidad de Escalamiento de privilegios en Cisco Application Policy Infrastructure Controlle.

CVE-2021-1579: Vulnerabilidad de Escalamiento de privilegios en Cisco Application Policy Infrastructure Controller App.

CVE-2021-1587: Vulnerabilidad de Denegación de servicio en la función OAM de VXLAN en Cisco NX-OS.

CVE-2021-1588: Vulnerabilidad de Denegación de servicio en la función OAM de MPLS en Cisco NX-OS.

Productos Afectados

Cisco Nexus 9500 Series.
Cisco UCS 6400 Series Fabric Interconnects si están corriendo una version vulnerable del Cisco UCS Manager software.
Nexus 3000 Series Switches, Nexus 7000 Series Switches, Nexus 9000 Series Switches in standalone NX-OS mode, si corren una version vulnerable de Cisco NX-OS y tienen la función MPLS OAM activada.
Nexus 3000 Series Switches y Nexus 9000 Series Switches si corren una version vulnerable de Cisco NX-OS y tienen la función NGOAM activada.
QNX SDP 6.5.0SP1 y anteriores, QNX OS for Medical 1.1 y anteriores y QNX OS for Safety 1.0.1 y anteriores
Cisco Nexus Insights.
Cisco Identity Services Engine (ISE)
Cisco Prime Collaboration Provisioning
Cisco Prime Infrastructure
Cisco Evolved Programmable Network Manager
Cisco Enterprise NFV Infrastructure Software (NFVIS)
Cisco Firepower Device Manager (FDM)
Cisco NX-OS Software
Cisco Application Policy Infrastructure Controller (APIC)
Cisco Cloud APIC

Mitigación

Instalar las respectivas actualizaciones entregadas por el proveedor.

Enlaces

https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-nexus-acl-vrvQYPVe
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-nxos-login-blockfor-RwjGVEcu
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ucs-ssh-dos-MgvmyrQy

https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-capic-chvul-CKfGYBh8
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-capic-pesc-pkmGK4J
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-nxos-mpls-oam-dos-sGO9x5GM
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-nxos-ngoam-dos-LTDb9Hv
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-insight-infodis-2By2ZpBB
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ise-xss-4HnZFewr
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-prime-collab-xss-fQMDE5GO
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-prime-info-disc-nTU9FJ2
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-nfvis-g2DMVVh
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-fdm-rce-Rx6vVurq
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20190515-nxos-pyth-escal
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-capic-mdvul-HBsJBuvW
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-capic-scss-bFT75YrM
https://cve.mitre.org/cgi-bin/cvename.cgi?name=
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-1727
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-1518
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-1578
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-1579
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-1580
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-1581
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-1582
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-1587
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-1588
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-1590
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-1591
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-1592
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-22156
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-34732
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-34733
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-34746
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-34759
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-34765

CSIRT Gobierno de Chile

Firmado digitalmente por CSIRT Gobierno de Chile
Fecha: 2021.09.02 16:44:21 -04'00'