Alerta de Seguridad Cibernética

Alerta de seguridad cibernética	9VSA22-00634-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Moderado
TLP	Blanco
Fecha de lanzamiento original	11 de mayo de 2022
Última revisión	11 de mayo 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 la información que comparte la información de nuevas vulnerabilidades entregada por Cisco para varios de sus productos.

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

Vulnerabilidades

CVE-2022-20764
CVE-2022-20794
CVE-2022-20796
CVE-2022-20785
CVE-2022-20770
CVE-2022-20771
CVE-2022-20734
CVE-2022-20799
CVE-2022-20801
CVE-2022-20753

Impacto

Todas estas vulnerabilidades son consideradas por Cisco como de riesgo moderado.

Productos afectados

RV340 Dual WAN Gigabit VPN Routers
RV340W Dual WAN Gigabit Wireless-AC VPN Routers
RV345 Dual WAN Gigabit VPN Routers
RV345P Dual WAN Gigabit POE VPN Routers
TelePresence CE Software
RoomOS Software in Cloud-Aware On-Premises, que se basa en la nube
Secure Endpoint, ex Advanced Malware Protection (AMP) for Endpoints, for Linux

Secure Endpoint, ex AMP for Endpoints, for MacOS
Secure Endpoint, formerly AMP for Endpoints, for Windows
Cisco SD-WAN vManage Software Release 20.6 y 20.7.

Mitigación

Instalar las respectivas actualizaciones entregadas por el proveedor.

Enlaces

https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-clamav-dos-vL9x58p4
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-clamav-html-XAuOK8mR
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-clamav-dos-prVGcHLd
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-clamav-dos-ZAZBwRVG
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-smb-rv-cmd-inj-8Pv9JMJD
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ROS-DOS-X7H7XhkK
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-20764
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-20794
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-20796
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-20785
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-20770
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-20771
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-20734
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-20799
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-20801
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-20753