ALERTA: AFECTACIÓN A EQUIPOS CISCO (22/SEPTIEMBRE/2021)

Investigadores alertan de vulnerabilidades en equipos CISCO.

Introducción

El Centro de Respuesta a Incidentes Informáticos de la ARCOTEL – EcuCERT, dentro de su gestión y como parte del apoyo recibió de su red de confianza nacional la notificación de vulnerabilidades asociadas a productos CISCO que se listan a continuación:

Tipo de incidente / Id de aviso	Afectación	Productos afectados	ID CVE	Puntaje base CVSS	Nivel de Impacto
Software Cisco IOS XE para controladores inalámbricos de la familia Catalyst 9000 Vulnerabilidad de ejecución remota de código CAPWAP. **Cisco-sa-ewlc-capwap-rce-LYgj8Kf**	CAPWAP podría permitir que un atacante remoto no autenticado ejecute código arbitrario con privilegios administrativos o cause una denegación de servicio (DoS) condición en un dispositivo afectado.	• Controlador inalámbrico integrado Catalyst 9800 para switches de las series Catalyst 9300, 9400 y 9500 • Controladores inalámbricos de la serie Catalyst 9800 • Controladores inalámbricos Catalyst 9800-CL para la nube • Controlador inalámbrico integrado en puntos de acceso Catalyst	CVE-2021-34770	10	Crítico
Vulnerabilidad de desbordamiento de búfer del software Cisco IOS XE SD-WAN. **Cisco-sa-iosxesdwan-rbuffover-vE2OB6tp**	Vulnerabilidad en el proceso vDaemon en el software Cisco IOS XE SD-WAN podría permitir que un atacante remoto no autenticado provoque un desbordamiento de búfer en un dispositivo afectado.	• Enrutadores de servicios integrados (ISR) de la serie 1000. • ISR de la serie 4000 • Enrutadores de servicios de agregación de la serie ASR 1000 • Enrutador de servicios en la nube serie 1000V	CVE-2021-34727	9,8	Crítico

Tipo de incidente / Id de aviso	Afectación	Productos afectados	ID CVE	Puntaje base CVSS	Nivel de Impacto
Vulnerabilidad de omisión de autenticación del software Cisco IOS XE NETCONF y RESTCONF. **Cisco-sa-aaa-Yx47ZT8Q**	Podría permitir que un atacante remoto no autenticado omita la autenticación NETCONF o RESTCONF y realice una de las siguientes acciones: • Instalar, manipular o eliminar la configuración de un dispositivo afectado • Causar daños en la memoria que resulten en una denegación de servicio (DoS) en un dispositivo afectado	Esta vulnerabilidad afecta al software Cisco IOS XE si se ejecuta en modo autónomo o de controlador y al software Cisco IOS XE SD-WAN. Para que cualquiera de los dos se vea afectado, se debe configurar todo lo siguiente: • AAA • NETCONF, RESTCONF o ambos • habilitar contraseña sin **enable secret**	CVE-2021-1619	9,8	Crítico
Vulnerabilidad de denegación de servicio de los puntos de acceso de Catalyst, del Controlador inalámbrico integrado de Cisco. **Cisco-sa-iosxe-ewc-dos-g6JruHRT**	Podría permitir que un atacante remoto no autenticado cause una condición de denegación de servicio (DoS) en un AP afectado.	• Esta vulnerabilidad afecta al software Cisco EWC para los AP Catalyst.	CVE-2021-1615	8,6	Alto
Vulnerabilidades de denegación de servicio CAPWAP para controladores inalámbricos de la familia Catalyst 9000. **Cisco-sa-ewlc-capwap-dos-gmNjdKOY**	Podrían permitir que un atacante remoto no autenticado cause una condición de denegación de servicio (DoS) en un dispositivo afectado.	• Controlador inalámbrico integrado Catalyst 9800 para switches de las series Catalyst 9300, 9400 y 9500 • Controladores inalámbricos de la serie Catalyst 9800 • Controladores inalámbricos Catalyst 9800-CL para la nube • Controlador inalámbrico integrado en puntos de acceso Catalyst	CVE-2021-1565 CVE-2021-34768 CVE-2021-34769	8,6	Alto
Vulnerabilidad de denegación de servicio EoGRE para los controladores inalámbricos de la serie Catalyst 9800	Podría permitir que un atacante remoto no autenticado cause una condición de denegación de servicio (DoS) en un dispositivo afectado. Un atacante podría	• Controlador inalámbrico integrado Catalyst 9800 para switches de las series Catalyst 9300, 9400 y 9500 • Controladores inalámbricos de la serie Catalyst 9800	CVE-2021-1611	8,6	Alto

Tipo de incidente / Id de aviso	Afectación	Productos afectados	ID CVE	Puntaje base CVSS	Nivel de Impacto
Cisco-sa-ewlc-gre-6u4ELzAT	aprovechar esta vulnerabilidad enviando paquetes maliciosos al dispositivo afectado. Un exploit exitoso podría permitir al atacante hacer que el dispositivo se recargue, lo que resultaría en una condición de DoS.	• Controlador inalámbrico Catalyst 9800 para la nube • Controlador inalámbrico integrado en puntos de acceso Catalyst			
Vulnerabilidad de denegación de servicio de servicio de política abierta común para routers de banda ancha convergentes Cisco cBR-8 **cisco-sa-cbr8-cops-Vc2ZsJSx**	Podría permitir que un atacante remoto no autenticado provoque el agotamiento de los recursos, lo que resultará en una condición de denegación de servicio (DoS). Esta vulnerabilidad se debe a una condición de interbloqueo en el código al procesar paquetes COPS bajo ciertas condiciones. Un atacante podría aprovechar esta vulnerabilidad enviando paquetes COPS con altas tasas de ráfaga a un dispositivo afectado. Un exploit exitoso podría permitir que el atacante haga que la CPU consuma recursos excesivos, lo que evita que otros procesos del plano de control obtengan recursos y dé como resultado un DoS.	Esta vulnerabilidad afecta a los routers de banda ancha convergente Cisco cBR-8 si ejecutan una versión del software Cisco IOS XE anterior a la versión 16.12.1z1 o la versión 17.3.1xy tienen la función COPS habilitada. El COPS escuchará cuando se cumpla alguna de las siguientes condiciones: • El puerto COPS TCP 2126 se abrirá con el comando packetcable • COPS puerto TCP 3918 se abrirá con multimedia de PacketCable comando.	CVE-2021-1622	8,6	Alto

Referencia

Cisco. Cisco Event Response: September 2021 Semiannual Cisco IOS and IOS XE Software Security Advisory Bundled Publication. (22 de septiembre de 2021). Recuperado el 22 de septiembre de 2021. Disponible en https://tools.cisco.com/security/center/viewErp.x?alertId=ERP-74581