CONCIBER
Comité Nacional de Seguridad Cibernética

ALERTA

Vulnerabilidad Crítica en Routers Linksys

Fecha: 10/01/2023

Problemática: Vulnerabilidades Críticas en Routers Linksys

Correlativo: AC-0009

Institución / Sector: Instituciones Públicas y Privadas

CONTEXTO

El equipo seguridad cibernética de Cisco Systems emitieron una alerta de seguridad por 3 vulnerabilidades en los ROUTERS de Cisco Small Business RV Series. Las vulnerabilidades CVE (Vulnerabilidades y Exposiciones Comunes) han sido identificadas como: CVE-2022-20827, CVE-2022-20841 y CVE-2022-20842 y han sido clasificadas como críticas debido al efecto que causaría la explotación de las mismas.

SITUACIÓN

CVE-2022-20842: Vulnerabilidad de ejecución remota de código y denegación de servicio de los routers de la serie RV de Cisco Small Business: Una vulnerabilidad en la interfaz de administración basada en web de los enrutadores Cisco RV340, RV340W, RV345 y RV345P Dual WAN Gigabit VPN podría permitir que un atacante remoto no autenticado ejecute código arbitrario o que un dispositivo afectado se reinicie inesperadamente, lo que resultaría en una denegación de servicio (DoS) condición.

CVE-2022-20827: Vulnerabilidad de inyección de comando de actualización de base de datos de filtro web de enrutadores de la serie RV de Cisco Small Business. Una vulnerabilidad en la función de actualización de la base de datos del filtro web de los enrutadores de las series RV160, RV260, RV340 y RV345 de Cisco Small Business podría permitir que un atacante remoto no autenticado realice una inyección de comando y ejecute comandos en el sistema operativo subyacente con privilegios de root .

CVE-2022-20841: Vulnerabilidad de inyección de comando Plug and Play abierta de los routers de la serie RV de Cisco Small Business.Una vulnerabilidad en el módulo Open Plug and Play (PnP) de los enrutadores de las series RV160, RV260, RV340 y RV345 de Cisco Small Business podría permitir que un atacante remoto no autenticado inyecte y ejecute comandos arbitrarios en el sistema operativo subyacente. Esta vulnerabilidad se debe a una validación insuficiente de la entrada proporcionada por el usuario. Un atacante podría aprovechar esta vulnerabilidad enviando información maliciosa a un dispositivo afectado. Una explotación exitosa podría permitir que el atacante ejecute comandos arbitrarios en el sistema operativo Linux subyacente.

Nivel de priorización

Prioridad Urgente / No Urgente	Actualización Seguimiento/Preventiva/Resiliente
Urgente	Preventiva

Matriz de Evaluación

Riesgo Alto/ Medio/ Bajo	Nivel de Afectación		
	Integridad	Disponibilidad	Confidencialidad
Alto	Alta	Alta	Alta

RECOMENDACIONES

Cisco Systems recomienda encarecidamente a los usuarios y administradores de sistemas que apliquen los parches de seguridad emitidos por el fabricante con el fin de evitar la exposición a ataques externos y la toma de control de los sistemas informáticos.

Por el momento, se desconocen medidas de mitigación alternativas a las propias actualizaciones lanzadas por Cisco para solucionar estas vulnerabilidades.

DICCIONARIO DE DATOS

1. Cifrado: Operación o función matemática utilizada en combinación con una clave que se aplica a un texto en claro y permite obtener un texto cifrado (o descifrarlo) garantizando la confidencialidad e integridad de la información contenida.
2. Código arbitrario: Hace referencia, en el campo de la seguridad informática, a la capacidad de un atacante para ejecutar comandos o inyectar código en una aplicación, aprovechando generalmente alguna vulnerabilidad.
3. Vulnerabilidad: Fallos de seguridad detectados en programas y sistemas que aprovechan los ciberdelincuentes para realizar ataques.

REFERENCIAS

1. Reporte Vulnerabilidad Cisco https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-mult-vuln-CbVp4SUR
2. https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-mult-vuln-CbVp4SUR
3. https://www.bleepingcomputer.com/news/security/cisco-fixes-critical-remote-code-execution-bug-in-vpn-routers/