Cisco lanzó el miércoles parches para abordar ocho vulnerabilidades de seguridad, tres de las cuales podrían ser armadas por un atacante no autenticado para obtener la ejecución remota de código (RCE) o causar una condición de denegación de servicio (DoS) en los dispositivos afectados.

La vulnerabilidad más crítica afecta a los enrutadores de las series RV160, RV260, RV340 y RV345 de Cisco Small Business. Rastreada como CVE-2022-20842 (puntuación CVSS: 9.8), la debilidad se deriva de una validación insuficiente de la entrada proporcionada por el usuario a la interfaz de administración basada en web de los dispositivos.

> *«Un atacante podría explotar esta vulnerabilidad enviando una entrada HTTP manipulada a un dispositivo afectado. Una explotación exitosa podría permitir que el atacante ejecute código arbitrario como usuario raíz en el sistema operativo subyacente o hacer que el dispositivo se recargue, lo que resultaría en una condición DoS»,* dijo Cisco en un aviso.

Una segunda vulnerabilidad se relaciona con una vulnerabilidad de inyección de comandos que reside en la función de actualización de la base de datos del filtro web de los routers (CVE-2022-20827, puntaje CVSS: 9.0), que podría ser explotada por un adversario para inyectar y ejecutar comandos arbitrarios en el sistema operativo subyacente con privilegios de root.

La tercera vulnerabilidad relacionada con router (CVE-2022-20841, puntaje CVSS: 8.0) también es un error de inyección de comandos en el módulo Open Plug-n-Play (PnP), que podría abusarse enviando una entrada maliciosa para lograr ejecución de código en el host Linux de destino.

> *«Para explotar esta vulnerabilidad, un atacante debe aprovechar una posición de hombre en el medio o tener un punto de apoyo establecido en un dispositivo de red específico que esté conectado al enrutador afectado»,* dijo Cisco.

Cisco también corrigió cinco fallas de seguridad media que afectan a Webex Meetings, Identity Services Engine, Unified Communications Manager y BroadWorks Application Delivery Platform.

La compañía no ofreció soluciones para remediar los problemas y agregó que no hay evidencia de que estas vulnerabilidades se exploten en la naturaleza.