Cisco implementó soluciones para múltiples vulnerabilidades críticas en la interfaz de administración basada en la web de los enrutadores para pequeñas empresas, que podrían permitir que un atacante remoto no autenticado ejecute código arbitrario como usuario root en un dispositivo afectado.

Las vulnerabilidades, rastreadas como CVE-2021-1289 hasta CVE-2021-1295, impactan en los routers VPN RV160, RV160W, RV260, RV260P y RV260W, que ejecutan una versión de firmware anterior a la versión 1.0.01.02.

Junto con las tres vulnerabilidades mencionadas antes, también se lanzaron parches para dos fallas de escritura de archivos arbitrarias (CVE-2021-1296 y CVE-2021-1297) que afectan al mismo conjunto de routers VPN que podrían haber hecho posible que un atacante sobrescribiera archivos arbitrarios en el sistema vulnerable.

Las nueve vulnerabilidades fueron informadas al fabricante de equipos de red por el investigador de seguridad Takeshi Shiomitsu, quien previamente descubrió fallas críticas similares en los enrutadores RV110W, RV130W y RV215W, que podrían aprovecharse para ataques de ejecución remota de código (RCE).

Cisco proporciono algunos detalles para las vulnerabilidades:

- CVE-2021-1289, CVE-2021-1290, CVE-2021-1291, CVE-2021-1292, CVE-2021-1293, CVE-2021-1294 y CVE-2021-1295: Son el resultado de una validación incorrecta de solicitudes HTTP, lo que permite a un atacante crear una solicitud HTTP especialmente diseñada para la interfaz de administración basada en web y lograr RCE.
- CVE-2021-1296 y CVE-2021-1297: Se deben a una validación de entrada insuficiente, lo que permite a un atacante aprovechar estas fallas utilizando la interfaz de administración basada en web para cargar un archivo en una ubicación a la que no debería tener acceso.

Por separado, otro conjunto de 5 vulnerabilidades (CVE-2021-1314 a CVE-2021-1318) en la interfaz de administración basada en web de los enrutadores RV016, RV042, RV042G, RV082,

RV320 y RV325 de Small Business, podrían haber otorgado al atacante la capacidad de inyectar comandos arbitrarios en los enrutadores que se ejecutan con privilegios de root.

Finalmente, Cisco abordó 30 vulnerabilidades adicionales (CVE-2021-1319 a CVE-2021-1348), que afectan al mismo conjunto de productos, que podrían permitir que un atacante remoto autenticado ejecute código arbitrario e incluso, provoque una condición de denegación de servicio.

> *«Para explotar estas vulnerabilidades, un atacante necesitaría tener credenciales de administrador válidas en el dispositivo afectado»,* dijo Cisco en un aviso publicado el 3 de febrero.

Kai Cheng, del Instituto de Ingeniería de la Información, que forma parte de la Academia de Ciencias de China, fue quien informó sobre las 35 vulnerabilidades en la interfaz de administración del enrutador.

La compañía también mencionó que no ha existido evidencia de intentos de explotación activos en la naturaleza para ninguno de los defectos, ni existen soluciones que aborden las vulnerabilidades.