Cisco Systems implementó correcciones para una falla de seguridad crítica que afecta al Administrador de Configuración de Redundancia (RCM) para el software Cisco StarOS, que podría ser armado por un atacante remoto no autenticado para ejecutar código arbitrario y apoderarse de máquinas vulnerables.

Rastreada como CVE-2022-20649, con puntaje CVSS de 9.0, la vulnerabilidad se deriva del hecho de que el modo de depuración se habilitó incorrectamente para servicios específicos.

> *«Un atacante podría explotar esta vulnerabilidad conectándose al dispositivo y navegando al servicio con el modo de depuración habilitado. Una explotación exitosa podría permitir que el atacante ejecute comandos arbitrarios como usuario raíz»*, dijo Cisco.

Sin embargo, el fabricante de equipos de red dijo que el adversario tendría que realizar un reconocimiento detallado para permitir el acceso no autenticado a los dispositivos vulnerables.

Al afirmar que la vulnerabilidad se descubrió durante las pruebas de seguridad internas, Cisco dijo que no encontró evidencia de explotación activa en ataques maliciosos.

Además de esto, la compañía también corrigió otras vulnerabilidades:

- CVE-2022-20648, con puntaje CVSS de 5.3: Vulnerabilidad de divulgación de información de depuración de Cisco RCM.
- CVE-2022-20685, con puntaje CVSS de 7.5: Vulnerabilidad de denegación Modbus Snort de varios productos de Cisco.
- CVE-2022-20655, con puntaje CVSS de 8.8: Vulnerabilidad de inyección de comandos CLI de ConfD.

Cisco explicó que CVE-2022-20655 se debe a una *«validación insuficiente de un argumento de proceso»* en un dispositivo afectado.

> *«Un atacante podría explotar estar vulnerabilidad inyectando comandos durante la ejecución de este proceso. Una explotación exitosa podría permitir que el atacante ejecute comandos arbitrarios en el sistema operativo subyacente con los privilegios del proceso del marco de administración, que comúnmente son privilegios de root»,* dijo la compañía.