Cisco ha lanzado actualizaciones para resolver una grave vulnerabilidad de seguridad que afecta a Emergency Responder y que permite a atacantes remotos no autenticados ingresar a sistemas vulnerables utilizando credenciales incrustadas en el código.

Esta vulnerabilidad, identificada como CVE-2023-20101 (con una calificación CVSS de 9.8), se debe a la existencia de credenciales de usuario estáticas para la cuenta root que la empresa ha indicado que normalmente se reservan para su uso durante el desarrollo.

> Cisco señaló en un comunicado: *«Un atacante podría aprovechar esta vulnerabilidad utilizando la cuenta para iniciar sesión en un sistema afectado. Una explotación exitosa podría permitir que el atacante inicie sesión en el sistema afectado y ejecute comandos arbitrarios como usuario root.»*

Este problema afecta a Cisco Emergency Responder Release 12.5(1)SU4 y ha sido solucionado en la versión 12.5(1)SU5. Las otras versiones del producto no se ven afectadas por esta falla.

La empresa líder en equipos de red informó que descubrió este problema durante pruebas internas de seguridad y que no tiene conocimiento de que se haya utilizado maliciosamente esta vulnerabilidad en la práctica.

Esta divulgación se produce menos de una semana después de que Cisco advirtiera sobre intentos de aprovechar una vulnerabilidad de seguridad en su software IOS e IOS XE (CVE-2023-20109, con una calificación CVSS de 6.6), que podría permitir que un atacante remoto autenticado logre la ejecución de código remoto en sistemas afectados.

Si no existen soluciones temporales disponibles, se recomienda encarecidamente a los clientes que actualicen a la versión más reciente para reducir el riesgo de posibles amenazas.