La empresa de ciberseguridad Acronis ha informado sobre una vulnerabilidad crítica en su producto Cyber Infrastructure (ACI), la cual ya ha sido parcheada pero había sido explotada en el entorno real.

La vulnerabilidad, identificada como CVE-2023-45249 y con una puntuación CVSS de 9,8, implica la ejecución remota de código debido al uso de contraseñas predeterminadas.

Las versiones afectadas de Acronis Cyber Infrastructure (ACI) son:

- Versión anterior a la 5.0.1-61
- Versión anterior a la 5.1.1-71
- Versión anterior a la 5.2.1-69
- Versión anterior a la 5.3.1-53
- Versión anterior a la 5.4.4-132

El problema se ha solucionado en las versiones 5.4 actualización 4.2, 5.2 actualización 1.3, 5.3 actualización 1.3, 5.0 actualización 1.4 y 5.1 actualización 1.2, publicadas a finales de octubre de 2023.

No se han proporcionado detalles sobre cómo se está explotando esta vulnerabilidad en ataques cibernéticos reales ni sobre los actores de amenazas responsables. Sin embargo, la empresa suiza reconoció la explotación activa de esta vulnerabilidad en un aviso actualizado la semana pasada.

> *«Se sabe que esta vulnerabilidad se está explotando en la naturaleza»*, indicó.

Se recomienda a los usuarios de las versiones afectadas de ACI que actualicen a la versión más reciente para reducir las posibles amenazas.