

Alerta de seguridad cibernética	9VSA21-00352-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Medio
TLP	Blanco
Fecha de lanzamiento original	6 de enero de 2021
Última revisión	6 de enero de 2021

NOTIFICACIÓN

La información consignada en el presente informe es producto del análisis de múltiples fuentes, de terceras partes, del propio fabricante e investigación propia del equipo CSIRT. La información contenida en los informes o comunicados está afecta a actualizaciones.

Resumen

El Equipo de Respuesta ante Incidentes de Seguridad Informática, CSIRT, comparte la información entregada por IBM sobre una serie de vulnerabilidades que afectan al IBM Cloud Pak System.

Este informe incluye las medidas de mitigación, consistentes en instalar la última actualización de los productos afectados.

Vulnerabilidades

CVE-2020-4917
CVE-2020-4928
CVE-2020-4919
CVE-2020-4918
CVE-2020-4916
CVE-2020-4913
CVE-2020-4912
CVE-2020-4910
CVE-2020-4909

Impacto

Estas vulnerabilidades son categorizadas como de riesgo medio. Las que aparecen como más riesgosas son dos de ellas, CVE-2020-4919 y CVE-2020-4912.

CVE-2020-4919, debido a un error de invalidación de sesión, hace posible a un atacante remoto comprometer el sistema objetivo. La compañía explica que IBM Cloud Pak System “tiene controles de logout insuficientes, lo que podría permitir a un usuario autenticado privilegiado hacerse pasar por otro usuario en el sistema”.

Por su parte, CVE-2020-4912 permite a un atacante remoto escalar privilegios en el sistema, a causa de que la aplicación no impone las restricciones de seguridad apropiadas de manera correcta.

Productos Afectados

IBM Cloud Pak System, versiones 2.3.0.1 a 2.3.3.2.

Mitigación

Instalar las actualizaciones del sitio del proveedor.

Enlaces

<https://www.ibm.com/support/pages/node/6393554>

<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-4917>

<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-4928>

<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-4919>

<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-4918>

<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-4916>

<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-4913>

<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-4912>

<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-4910>

<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-4909>