Se han desvelado más pormenores acerca de un conjunto de vulnerabilidades de cross-site scripting (XSS) en el servicio de análisis de código abierto de Microsoft Azure HDInsight, las cuales han sido corregidas y que podrían ser utilizadas por un actor malicioso para llevar a cabo actividades perjudiciales.

> *«Las vulnerabilidades identificadas incluyeron seis XSS almacenados y dos XSS reflejados, cada uno de los cuales podría ser explotado para llevar a cabo acciones no autorizadas, que van desde el acceso a datos hasta la toma de sesiones y la entrega de payloads maliciosos»*, informó Lidor Ben Shitrit, investigador de seguridad de Orca.

Microsoft abordó estos problemas como parte de sus actualizaciones de *«Patch Tuesday»* para agosto de 2023.

Esta divulgación se produce tres meses después de que se informara de deficiencias similares en Azure Bastion y Azure Container Registry, que podrían haber sido aprovechadas para obtener acceso no autorizado y realizar modificaciones en los datos.

La lista de fallas es la siguiente:

- CVE-2023-35393 (puntuación CVSS: 4.5) – Vulnerabilidad de suplantación de identidad en Azure Apache Hive.
- CVE-2023-35394 (puntuación CVSS: 4.6) – Vulnerabilidad de suplantación de identidad en Azure HDInsight Jupyter Notebook.
- CVE-2023-36877 (puntuación CVSS: 4.5) – Vulnerabilidad de suplantación de identidad en Azure Apache Oozie.
- CVE-2023-36881 (puntuación CVSS: 4.5) – Vulnerabilidad de suplantación de identidad en Azure Apache Ambari.
- CVE-2023-38188 (puntuación CVSS: 4.5) – Vulnerabilidad de suplantación de identidad en Azure Apache Hadoop.

Microsoft señaló en sus avisos sobre los errores que *«un atacante tendría que enviar un archivo malicioso a la víctima, el cual la víctima tendría que ejecutar. Un atacante autorizado con privilegios de invitado debe enviar a la víctima un sitio malicioso y convencerla de que lo abra».*

Los ataques XSS se producen cuando un adversario inyecta scripts maliciosos en un sitio web legítimo, los cuales se ejecutan en los navegadores web de las víctimas cuando visitan el sitio. Mientras que el XSS reflejado se dirige a usuarios que son engañados para hacer clic en un enlace fraudulento, el XSS almacenado está incrustado en una página web y afecta a todos los usuarios que la visitan.

La empresa de seguridad en la nube indicó que todas estas fallas derivan de una falta de saneamiento adecuado de la entrada, lo que permite que caracteres maliciosos sean representados al cargar el panel de control.

Ben Shitrit hizo hincapié en la importancia de que las organizaciones implementen una validación adecuada de la entrada y la codificación de la salida para *«garantizar que los datos generados por el usuario sean debidamente purificados antes de ser mostrados en las páginas web».*