Alerta de seguridad cibernética	9VSA20-00267-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	09 de julio de 2020
Última revisión	09 de julio de 2020

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 obtenida de Apache Spark respecto a vulnerabilidad que permite la evasión de medidas de autenticación. El presente informe incluye la respectiva medida de mitigación.

Vulnerabilidad

CVE-2020-9480

CVE-2020-9480

El maestro de un administrador de recursos independientes podía configurarse para requerir autenticación (spark.autheticate) a través de una llave compartida. Sin embargo, al activarlo, un "RPC" especialmente diseñado para el maestro podía ejecutar exitosamente recursos de la aplicación en el cluster Spark, aun sin esta llave. Esto podía utilizarse para ejecutar comandos de Shell en la máquina afectada.
Esta vulnerabilidad no afecta a clusters que utilicen otros administradores de recursos, como YARN, Mesos, etc.

Productos Afectados

Apache Spark versión 2.4.5 y anteriores.

Mitigaciones

Actualizar a la versión 2.4.6 o 3.0.0 de Apache Spark.

Enlaces

https://spark.apache.org/security.html#CVE-2020-9480
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-9480