Alerta de seguridad cibernética	9VSA20-00345-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	23 de diciembre de 2020
Última revisión	23 de diciembre 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 entregada por la MariaDB Foundation una vulnerabilidad que afecta a algunos de sus productos MariaDB. Este informe incluye la medida de mitigación, consistente en instalar la última actualización de los productos afectados.

Vulnerabilidad

CVE-2020-15180

Impacto

La vulnerabilidad CVE-2020-15180 es considerada de riesgo alto, ya que permite a un atacante remoto ejecutar comandos “shell” arbitrarios en el sistema objetivo.

Esta vulnerabilidad existe debido a una validación inapropiada de los datos ingresados por un usuario en el método “wsrep_sst_method” del componente “mysql-wsrep” de MariaDB. Un atacante remoto no autenticado puede pasar datos especialmente diseñados a la aplicación y ejecutar comandos de sistema operativo arbitrarios en el nodo cluster Galera. Una explotación exitosa de esta vulnerabilidad puede resultar en el compromiso completo del sistema vulnerable.

No se conoce de malware que explote esta vulnerabilidad.

Productos Afectados

Maria DB versiones desde la 10.1.0 a la 10.5.5.

Mitigación

Instalar las actualizaciones desde el sitio del proveedor.

Enlaces

https://bugzilla.redhat.com/show_bug.cgi?id=1894919

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-15180