Nro. Alerta:	EC-2022-17	CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS **ALERTA DE SEGURIDAD**	CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS ECUCERT
TLP:	TLP:BLANCO		
Fecha:	01-febrero-2022	**Vulnerabilidades en MariaDB**	Versión 1.0

I. DATOS GENERALES:

Clase de alerta: Vulnerabilidad
Tipo de incidente: Sistema Vulnerable
Nivel de riesgo: Media

II. ALERTA

MariaDB presenta diferentes vulnerabilidades afectando a diferentes versiones que van desde: 10.5.9 hasta la 10.6.5.

Figura 1.- Ilustración asociada a Maria DB
Fuente: General Electric

III. INTRODUCCIÓN

MariaDB es un sistema de gestión de base de datos, se encuentra entre las más populares. Está hecho por los desarrolladores originales de MySQL, es de código abierto y según su página WEB se garantiza que permanecerá como código abierto. Así mismo, es parte de la mayoría de las ofertas en la nube y el valor predeterminado en la mayoría de las distribuciones de Linux.

En este sentido, diferentes vulnerabilidades han sido detectadas en diferentes versiones de este sistema de gestión de base datos. Estas vulnerabilidades fueron publicadas el primero de febrero de 2022; a continuación, se mencionan las principales características de cada una de ellas.

Dirección: Av. Amazonas N40-71 y Gaspar de Villaroel
Código postal: 170501 / Quito-Ecuador
Teléfono: 593-2 2271 180 - www.arcotel.gob.ec

Nro. Alerta:	EC-2022-17	CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS **ALERTA DE SEGURIDAD**	CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS ECUCERT
TLP:	TLP:BLANCO		
Fecha:	01-febrero-2022	**Vulnerabilidades en MariaDB**	Versión 1.0

CVE ASOCIADO	DESCRIPCIÓN	LINK DE REFERENCIA
CVE-2021-46661	MariaDB hasta 10.5.9 permite un bloqueo de la aplicación en **find_field_in_tables** y **find_order_in_list** a través de una expresión de tabla común (CTE) no utilizada.	https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-46661
CVE-2021-46662	MariaDB hasta 10.5.9 permite un bloqueo de la aplicación **set_var.cc** a través de ciertos usos de una instrucción UPDATE junto con una subconsulta anidada.	https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-46662
CVE-2021-46663	MariaDB a través de 10.5.13 permite un bloqueo de la aplicación **ha_maria::extra** a través de ciertas declaraciones SELECT.	https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-46663
CVE-2021-46664	MariaDB hasta 10.5.9 permite un bloqueo de la aplicación en **sub_select_postjoin_aggr** para un valor NULL de aggr.	https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-46664
CVE-2021-46665	MariaDB hasta 10.5.9 permite un bloqueo de la aplicación **sql_parse.cc** debido a expectativas incorrectas de **used_tables.**	https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-46665
CVE-2021-46666	MariaDB anterior a 10.6.2 permite un bloqueo de la aplicación debido al mal manejo de un **pushdown** de una cláusula **HAVING** a una cláusula **WHERE**.	https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-46666
CVE-2021-46667	MariaDB anterior a 10.6.5 tiene un desbordamiento de enteros **sql_lex.cc**, lo que provoca un bloqueo de la aplicación	https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-46667
CVE-2021-46668	MariaDB hasta 10.5.9 permite que una aplicación se cuelgue a través de ciertas declaraciones SELECT DISTINCT largas que interactúan incorrectamente con las limitaciones de recursos del motor de almacenamiento para estructuras de datos temporales.	https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-46668
CVE-2021-46669	MariaDB hasta 10.5.9 permite a los atacantes activar **convert_const_to_int use-after-free** cuando se usa el tipo de datos BIGINT.	https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-46669

Tabla 1. Características vulnerabilidades.

Dirección: Av. Amazonas N40-71 y Gaspar de Villaroel
Código postal: 170501 / Quito-Ecuador
Teléfono: 593-2 2271 180 - www.arcotel.gob.ec

Nro. Alerta:	EC-2022-17	CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS **ALERTA DE SEGURIDAD**	CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS ECUCERT
TLP:	TLP:BLANCO		
Fecha:	01-febrero-2022	**Vulnerabilidades en MariaDB**	Versión 1.0

IV. VECTOR DE ATAQUE:

A continuación, se describen las características de las vulnerabilidades encontradas.

CVE ASOCIADO	DESCRIPCIÓN	IMPACTO	BUG REPORT
CVE-2021-46661	• Mediante la manipulación de un input desconocido se causa una vulnerabilidad de clase denegación de servicio. • El ataque puede ser realizado a través de la red. • La explotación no requiere ninguna forma de autentificación. • CVSS Meta Temp Score: 5.1	Repercusión sobre la disponibilidad.	https://jira.mariadb.org/browse/MDEV-25766
CVE-2021-46662			https://jira.mariadb.org/browse/MDEV-25637
CVE-2021-46663			https://jira.mariadb.org/browse/MDEV-26351
CVE-2021-46664			https://jira.mariadb.org/browse/MDEV-25761
CVE-2021-46665			https://jira.mariadb.org/browse/MDEV-25636
CVE-2021-46666			https://jira.mariadb.org/browse/MDEV-25635
CVE-2021-46667			https://jira.mariadb.org/browse/MDEV-26350
CVE-2021-46668	• CVSS Meta Temp Score: 4.8		https://jira.mariadb.org/browse/MDEV-25787
CVE-2021-46669	• CVSS Meta Temp Score: 7.0		https://jira.mariadb.org/browse/MDEV-25638

Tabla 2. Vector de Ataque e Impacto de las vulnerabilidades.

V. RECOMENDACIONES:

El EcuCert recomienda a su comunidad objetivo:

- Aplicar los parches de seguridad en cuanto se encuentren disponibles, con el fin de evitar la exposición a ataques externos.
- Instalar las actualizaciones oficiales de MariaDB cuando se encuentren disponibles.
- Prestar atención al funcionamiento de las aplicaciones afectadas.

Dirección: Av. Amazonas N40-71 y Gaspar de Villaroel
Código postal: 170501 / Quito-Ecuador
Teléfono: 593-2 2271 180 - www.arcotel.gob.ec

Nro. Alerta:	EC-2022-17	CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS **ALERTA DE SEGURIDAD**	CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS ECUCERT
TLP:	TLP:BLANCO		
Fecha:	01-febrero-2022	**Vulnerabilidades en MariaDB**	Versión 1.0

VI. REFERENCIAS:

MariaDB. (s.f.). *MariaDB*. Obtenido de https://mariadb.org/

MITRE, C. (01 de 02 de 2022). *CVE MITRE*. Obtenido de CVE MITRE: https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-46667

MITRE, C. (01 de 02 de 2022). *CVE MITRE*. Obtenido de CVE MITRE: https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-46662

MITRE, C. (01 de 02 de 2022). *CVE MITRE*. Obtenido de CVE MITRE: https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-46665

MITRE, C. (01 de 02 de 2022). *CVE MITRE*. Obtenido de CVE MITRE: https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-46667

MTIRE, C. (01 de 02 de 2022). *CVE MTIRE*. Obtenido de CVE MTIRE: https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-46661

MTIRE, C. (01 de 02 de 2022). *CVE MTIRE*. Obtenido de CVE MTIRE: https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-46663

MTIRE, C. (01 de 02 de 2022). *CVE MTIRE*. Obtenido de CVE MTIRE: https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-46664

MTIRE, C. (01 de 02 de 2022). *CVE MTIRE*. Obtenido de CVE MTIRE: https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-46666

MTIRE, C. (01 de 02 de 2022). *CVE MTIRE*. Obtenido de CVE MTIRE: https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-46668

MTIRE, C. (01 de 02 de 2022). *CVE MTIRE*. Obtenido de CVE MTIRE: https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-46669

Vuldb. (01 de 02 de 2022). *Vuldb*. Obtenido de Vuldb: https://vuldb.com/es/?id.192034

Vuldb. (01 de 02 de 2022). *Vuldb*. Obtenido de Vuldb: https://vuldb.com/es/?id.192035

Vuldb. (01 de 02 de 2022). *Vuldb*. Obtenido de Vuldb: https://vuldb.com/es/?id.192036

Vuldb. (01 de 02 de 2022). *Vuldb*. Obtenido de Vuldb: https://vuldb.com/es/?id.192037

Vuldb. (01 de 02 de 2022). *Vuldb*. Obtenido de Vuldb: https://vuldb.com/?id.192038

Vuldb. (01 de 02 de 2022). *Vuldb*. Obtenido de Vuldb: https://vuldb.com/?id.192039

Vuldb. (01 de 02 de 2022). *Vuldb*. Obtenido de Vuldb: https://vuldb.com/?id.192040

Vuldb. (01 de 02 de 2022). *Vuldb*. Obtenido de Vuldb: https://vuldb.com/?id.192033

Vuldb. (01 de 02 de 2022). *Vuldb*. Obtenido de Vuldb: https://vuldb.com/zh/?id.192041

Dirección: Av. Amazonas N40-71 y Gaspar de Villaroel
Código postal: 170501 / Quito-Ecuador
Teléfono: 593-2 2271 180 - www.arcotel.gob.ec