Alerta de seguridad informática	9VSA20-00133-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	05 de febrero de 2020
Última revisión	05 de febrero 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 información obtenida del github de MariaDB, referente a una vulnerabilidad que afecta a su motor de base de datos, la cual de ser explotada permitiría a un atacante escalar privilegios en el sistema afectado. Este informe incluye la respectiva mitigación.

Vulnerabilidad

CVE-2020-7221

Impacto

La vulnerabilidad permite a un usuario remoto escalar privilegios en el sistema.
La vulnerabilidad existe en el script "mysql_install_db" debido a que "chown" y "chmod" (herramientas para modificar quiénes pueden hacer uso de archivos y directorios) se realizan de manera insegura, como lo demuestra un ataque de enlace simbólico en “chmod 04755” de “auth_pam_tool_dir / auth_pam_tool”.
La explotación de esta vulnerabilidad permitiría a un usuario remoto obtener privilegios máximos en el sistema vulnerable.

Productos Afectados

MariaDB versiones: 10.4.7, 10.4.8, 10.4.9, 10.4.10 y 10.4.11.

Mitigación

Aplicar las actualizaciones publicadas por el fabricante.

Enlaces

https://www.cybersecurity-help.cz/vdb/SB2020020507
https://github.com/MariaDB/server/commit/9d18b6246755472c8324bf3e20e234e08ac45618
https://cve.mitre.org/cgi-bin/cvename.cgi?name= CVE-2020-7221

CSIRT Gobierno de Chile
Firmado digitalmente por CSIRT Gobierno de Chile
Fecha: 2020.02.05 11:08:20 -03'00'