I. DATOS GENERALES:

Clase de alerta: Vulnerabilidad crítica en cPanel y WHM
Tipo de Incidente: Vulnerabilidad de escalamiento de privilegios que permite la ejecución de SQL con privilegios de root en bases de datos (CVE-2026-58048)
Nivel de riesgo: Alta

II. ALERTA

Figura 1.- Vulnerabilidad crítica en cPanel y WHM permite ejecución de SQL con privilegios de root (CVE-2026-58048) - figura referencial

Se ha identificado una vulnerabilidad crítica en **cPanel** y **WHM (Web Host Manager)**, registrada como **CVE-2026-58048**, que podría permitir a un usuario autenticado con acceso a una cuenta de hosting ejecutar consultas SQL con privilegios elevados sobre el servidor de bases de datos **MySQL/MariaDB.**

III. INTRODUCCIÓN

La vulnerabilidad **CVE-2026-58048** está clasificada bajo **CWE-89 (SQL Injection)** y puede ser utilizada para realizar acciones que conduzcan al **escalamiento de privilegios** dentro de entornos que ejecutan **cPanel y WHM**. Su explotación requiere

que el atacante disponga de acceso válido a una cuenta de cPanel y acceso a una instancia de **MySQL o MariaDB** con privilegios elevados sobre el sistema de archivos. Bajo estas condiciones, el impacto puede escalar hasta comprometer completamente el servidor afectado.

Una explotación exitosa de esta vulnerabilidad, que afecta directamente a las funcionalidades de administración de bases de datos de cPanel y WHM, podría permitir el acceso no autorizado a información sensible almacenada en bases de datos de clientes, la modificación de usuarios y privilegios de bases de datos, la extracción de credenciales, la creación de procedimientos o desencadenadores (triggers) maliciosos, así como el acceso, lectura o manipulación de archivos del sistema mediante capacidades avanzadas de MySQL/MariaDB. En escenarios de compromiso avanzado, estas acciones podrían facilitar la ejecución de código arbitrario, la persistencia del atacante y el control total del servidor.

IV. VECTOR DE ATAQUE

Esta vulnerabilidad crítica en cPanel y WHM (CVE-2026-58048) posee una severidad CRITICAL con una puntuación CVSS:4.0 de 9.4 tipo /AV:N/AC:L/AT:N/PR:L/UI:N/VC:H/VI:H/VA:H/SC:H/SI:H/SA:H

V. IMPACTO

Producto	Versiones afectadas	Versiones corregidas (parcheadas)
cPanel y WHM	Todas las versiones compatibles anteriores a las actualizaciones de seguridad publicadas por el fabricante.	11.110.0.137 11.118.0.71 11.126.0.78 11.134.0.48 11.136.0.32 138.1.6 (WP2)

Tabla 1.- Sistemas afectados - Vulnerabilidad crítica en cPanel y WHM permite ejecución de SQL con privilegios de root (CVE-2026-58048)

VI. INDICADORES DE COMPROMISO

- Consultas SQL inusuales ejecutadas con privilegios elevados.
- Creación o modificación inesperada de usuarios de bases de datos.
- Accesos no autorizados a bases de datos de otros clientes.
- Registros anómalos en MySQL/MariaDB.
- Cambios inesperados en permisos de bases de datos.

VII. RECOMENDACIONES:

- Actualizar inmediatamente cPanel y WHM a la versión corregida por el fabricante.
- Aplicar todos los parches de seguridad publicados por cPanel.
- Revisar los registros de MySQL/MariaDB para identificar actividades inusuales.
- Auditar los permisos de los usuarios de bases de datos.
- Restringir el acceso administrativo únicamente al personal autorizado.
- Implementar monitoreo continuo sobre las bases de datos.
- Realizar copias de seguridad antes de aplicar las actualizaciones.

VIII. DESCARGO DE RESPONSABILIDAD

- La información en la presente alerta se proporciona con fines informativos.
- Cualquier referencia a productos, procesos o servicios comerciales específicos, no constituye respaldo o recomendación por parte del EcuCERT a los mismos.
- La presente alerta no debe utilizarse con fines publicitarios o de patrocinio de productos.

IX. REFERENCIAS:

CPANEL (2026). Security: CVE-2026-58048 – Database Privilege Escalation**.** https://support.cpanel.net/hc/en-us/articles/42285745783703-Security-CVE-2026-58048-Database-Privilege-Escalation

DEVEL GROUP (2026). Vulnerabilidad crítica de escalada de privilegios en cPanel y WHM (CVE-2026-58048)**.** https://devel.group/blog/vulnerabilidad-critica-de-escalada-de-privilegios-en-cpanel-y-whm-cve-2026-58048/

THE HACKER NEWS (2026). New cPanel Critical Flaw Could Let Hosting Customers Execute SQL as Database Root**.** https://thehackernews.com/2026/08/new-cpanel-critical-flaw-could-let.html

CVE (2026). CVE-2026-58048**.** https://www.cve.org/CVERecord?id=CVE-2026-58048

NATIONAL VULNERABILITY DATABASE (NVD) (2026). CVE-2026-58048**.** https://nvd.nist.gov/vuln/detail/CVE-2026-58048