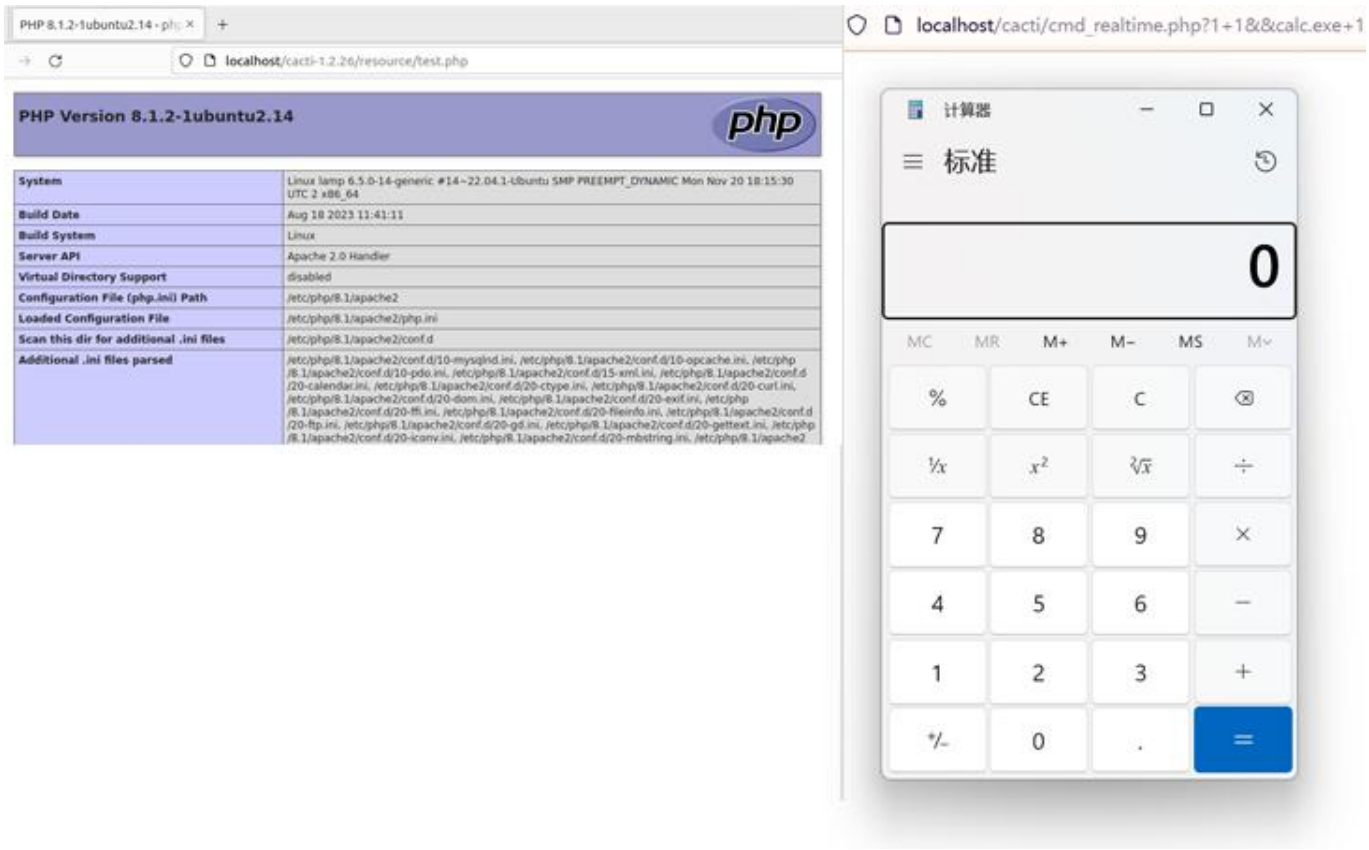
Los administradores del marco de gestión de redes y de gestión de fallos de código abierto Cacti han abordado una docena de fallos de seguridad, incluyendo dos problemas críticos que podrían resultar en la ejecución de código arbitrario.

A continuación, se enumeran las vulnerabilidades más graves:

- CVE-2024-25641 (puntuación CVSS: 9.1) – Una vulnerabilidad de escritura de archivo arbitraria en la función «Importar Paquete» que permite a los usuarios autenticados con el permiso «Importar Plantillas» ejecutar código PHP arbitrario en el servidor web, lo que resulta en la ejecución remota de código.
- CVE-2024-29895 (puntuación CVSS: 10.0) – Una vulnerabilidad de inyección de comandos que permite a cualquier usuario no autenticado ejecutar comandos arbitrarios en el servidor cuando la opción «register_argc_argv» de PHP está habilitada.



Cacti también ha abordado otras dos vulnerabilidades de alta gravedad que podrían resultar en la ejecución de código mediante inyección de SQL e inclusión de archivos:

- CVE-2024-31445 (puntuación CVSS: 8.8) – Una vulnerabilidad de inyección de SQL en api_automation.php que permite a usuarios autenticados realizar escalada de privilegios y ejecución remota de código.
- CVE-2024-31459 (puntuación CVSS: N/A) – Un problema de inclusión de archivos en el archivo «lib/plugin.php» que podría combinarse con vulnerabilidades de inyección de SQL para resultar en la ejecución remota de código.

Es importante destacar que 10 de los 12 fallos, con excepción de CVE-2024-29895 y CVE-2024-30268 (puntuación CVSS: 6.1), afectan a todas las versiones de Cacti, incluidas aquellas anteriores a la versión 1.2.26. Estos problemas han sido abordados en la versión 1.2.27 lanzada el 13 de mayo de 2024. Las otras dos vulnerabilidades afectan a las versiones de desarrollo 1.3.x.

Estos desarrollos llegan más de ocho meses después de la divulgación de otra vulnerabilidad crítica de inyección de SQL (CVE-2023-39361, puntuación CVSS: 9.8) que podría permitir a un atacante obtener permisos elevados y ejecutar código malicioso.

A principios de 2023, una tercera falla crítica rastreada como CVE-2022-46169 (puntuación CVSS: 9.8) fue objeto de explotación activa en la naturaleza, permitiendo a actores de amenazas comprometer servidores Cacti expuestos a Internet para entregar malware de botnet como MooBot y ShellBot.

Dado que hay exploits de prueba de concepto (PoC) disponibles públicamente para estas deficiencias (en las respectivas notificaciones de GitHub), se recomienda encarecidamente a los usuarios que tomen medidas para actualizar sus instancias a la última versión lo antes posible para mitigar posibles amenazas.