



Vulnerabilidades críticas en Cacti Framework podrían permitir a los hackers ejecutar código malicioso

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.

The image shows a browser window displaying the PHP version information for a server. The browser address bar shows the URL `localhost/cacti-1.2.26/resource/test.php`. The page title is "PHP Version 8.1.2-1ubuntu2.14". The PHP logo is visible in the top right corner. The main content is a table with system and configuration details.

System	Linux lamp 6.5.0-14-generic #14~22.04.1-Ubuntu SMP PREEMPT_DYNAMIC Mon Nov 20 18:15:30 UTC 2 x86_64
Build Date	Aug 18 2023 11:41:11
Build System	Linux
Server API	Apache 2.0 Handler
Virtual Directory Support	disabled
Configuration File (php.ini) Path	/etc/php/8.1/apache2
Loaded Configuration File	/etc/php/8.1/apache2/php.ini
Scan this dir for additional .ini files	/etc/php/8.1/apache2/conf.d
Additional .ini files parsed	/etc/php/8.1/apache2/conf.d/10-mysqlnd.ini, /etc/php/8.1/apache2/conf.d/10-opcache.ini, /etc/php/8.1/apache2/conf.d/10-pdo.ini, /etc/php/8.1/apache2/conf.d/15-xsl.ini, /etc/php/8.1/apache2/conf.d/20-calendar.ini, /etc/php/8.1/apache2/conf.d/20-ctype.ini, /etc/php/8.1/apache2/conf.d/20-curl.ini, /etc/php/8.1/apache2/conf.d/20-dbm.ini, /etc/php/8.1/apache2/conf.d/20-exif.ini, /etc/php/8.1/apache2/conf.d/20-ftp.ini, /etc/php/8.1/apache2/conf.d/20-gd.ini, /etc/php/8.1/apache2/conf.d/20-gettext.ini, /etc/php/8.1/apache2/conf.d/20-iconv.ini, /etc/php/8.1/apache2/conf.d/20-ldap.ini, /etc/php/8.1/apache2/conf.d/20-mbstring.ini, /etc/php/8.1/apache2/

Overlaid on the right side of the browser window is a Windows-style calculator application. The calculator is in Chinese, titled "计算器" (Calculator), and is set to "标准" (Standard) mode. The display shows the number "0". The calculator interface includes a numeric keypad, function keys (MC, MR, M+, M-, MS, Mv), and mathematical operators.



Vulnerabilidades críticas en Cacti Framework podrían permitir a los hackers ejecutar código malicioso

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.