BOLETÍN DE ALERTA

Boletín Nro.: 2023-40
Fecha de publicación: 08/09/2023
Tema: Vulnerabilidades permiten inyección SQL (*SQLi*) y escalamiento de privilegios en Cacti

Software afectado:

- Cacti, versiones anteriores a 1.2.25.

Descripción:

Se han reportado nuevos avisos de seguridad sobre múltiples vulnerabilidades que afectan a Cacti, que permitirían a un atacante realizar inyección *SQL* (*SQLi*) y escalamiento de privilegios, entre otros. Actualmente para estas vulnerabilidades existen pruebas de concepto (*PoC*) públicas. Lo cual supone la explotación inminente de los sistemas publicados en internet.

Las vulnerabilidades reportadas se componen de 1 (una) de severidad “Crítica”, 5 (cinco) de severidad “Alta”, 11 (once) de severidad “Media” y 1 (una) de severidad “Baja”. Las principales se detallan a continuación:

- CVE-2023-39361, de severidad “Crítica”, con puntuación asignada de 9.8. Esta vulnerabilidad de inyección *SQL* (*SQLi*) se debe a una falla de seguridad en la función *grow_right_pane_tree* tras el llamado al archivo *graph_view.php* de Cacti. Esto permitiría a un atacante a través del acceso de usuarios invitados sin autenticación, para obtener privilegios administrativos y también provocar ejecución remota de código (*RCE*) alterando el valor '*path_php_binary*' en la base de datos del sistema afectado.

- CVE-2023-39357, de severidad “Alta”, con puntuación asignada de 8.8. Esta vulnerabilidad de inyección *SQL* (*SQLi*) se debe a una falla de validación de datos de entrada del usuario en la función *sql_save* de Cacti. Esto permitiría a un atacante autenticado realizar escalamiento de privilegios, ejecución remota de código (*RCE*), y potencialmente comprometer la integridad y confidencialidad del sistema afectado.

- CVE-2023-39358, de severidad “Alta”, con puntuación asignada de 8.8. Esta vulnerabilidad de inyección *SQL* (*SQLi*) se debe a una falla de validación de datos de entrada del usuario en el archivo *reports_user.php* de Cacti. Esto permitiría a un atacante autenticado a través del archivo *ajax_get_branches* y el parametro *tree_id*, realizar escalamiento de privilegios a traves de la función *reports_get_branch_select*, ejecución remota de código (*RCE*), además de comprometer la integridad y confidencialidad del sistema afectado.

Puede acceder al listado completo de vulnerabilidades aquí.

Impacto:

La explotación exitosa de estas vulnerabilidades podría permitir a un atacante realizar inyección SQL (*SQLi*), escalamiento de privilegios y ejecución remota de código (*RCE*) en el sistema afectado.

Solución:

Recomendamos acceder a la actualización de seguridad correspondiente a través del siguiente enlace:

- https://github.com/Cacti/cacti/releases/tag/release%2F1.2.25

Información adicional:

- https://securityonline.info/cve-2023-39361-critical-sql-injection-vulnerability-found-in-cacti/#google_vignette
- https://nvd.nist.gov/vuln/detail/CVE-2023-39361
- https://nvd.nist.gov/vuln/detail/CVE-2023-39357
- https://nvd.nist.gov/vuln/detail/CVE-2023-39358
- https://github.com/Cacti/cacti/security/advisories/GHSA-6jhp-mgqg-fhqg
- https://github.com/Cacti/cacti/security/advisories/GHSA-gj95-7xr8-9p7g
- https://github.com/Cacti/cacti/security/advisories/GHSA-q4wh-3f9w-836h
- https://github.com/Cacti/cacti/releases/tag/release%2F1.2.25