BOLETÍN DE ALERTA

Boletín Nro.: 2023-04
Fecha de publicación: 13/01/2023
Tema: Vulnerabilidad de ejecución remota de código (*RCE)* en Cacti.

Las versiones afectadas son:

- Cacti, versión 1.2.22 y anteriores

Descripción:

Se ha reportado un nuevo aviso de seguridad sobre una vulnerabilidad que afecta a Cacti, que permitiría a un atacante no autenticado realizar ejecución de código arbitrario, omisión de autenticación, entre otros.

La vulnerabilidad identificada como CVE-2022-46169 de severidad "Crítica" y con puntuación asignada de 9.8. Esta vulnerabilidad de inyección de comandos se debe a una falla de control de autenticación en el archivo "*remote_agent.php*" del servidor de Cacti. Esto permitiría a un atacante no autenticado cuando se encuentre configurado en Cacti un componente "*poller_item*" con una acción del tipo "*POLLER_ACTION_SCRIPT_PHP*" realizar ejecución de comandos arbitrarios y ejecución remota de código (*RCE*) en el servidor afectado. Actualmente existe una prueba de concepto (*PoC)* pública.

Impacto:

La explotación exitosa de esta vulnerabilidad permitiría a un atacante no autenticado realizar evasión de autenticación e inyección de comandos en el sistema afectado.

Solución:

Recomendamos acceder a la actualización de seguridad correspondiente a través de la siguiente guía provista por Cacti:

- https://files.cacti.net/docs/html/upgrade.html

Información adicional:

- https://twitter.com/DragonJAR/status/1613195991334666241?t=o1vsx3yztULdZ3clUI9T8g&s=08
- https://www.sonarsource.com/blog/cacti-unauthenticated-remote-code-execution/
- https://nvd.nist.gov/vuln/detail/CVE-2022-46169
- https://github.com/Cacti/cacti/security/advisories/GHSA-6p93-p743-35gf