BOLETÍN DE ALERTA

Boletín Nro.: 2023-17
Fecha de publicación: 02/05/2023

Tema: Vulnerabilidad del tipo *reflected cross-site scripting* (*XSS*) en cPanel

Las versiones de cPanel afectadas son:

- cPanel, versiones anteriores a 11.109.9999.116, 11.108.0.13, 11.106.0.18 y 11.102.0.31.

Descripción:

Se ha reportado un nuevo aviso de seguridad sobre una vulnerabilidad del tipo *reflected cross-site scripting* (*XSS*) que afecta a cPanel, que permitiría a un atacante no autenticado ejecutar códigos JavaScript arbitrarios en casi todos los puertos de un servidor web y potencialmente secuestrar una sesión de cPanel. Actualmente para esta vulnerabilidad existe prueba de concepto (*PoC*) pública.

La vulnerabilidad identificada como CVE-2023-29489, sin severidad asignada aún. Esta vulnerabilidad del tipo *reflected cross-site scripting* (*XSS*) se debe a una falla de validación de entradas en el párametro *webcall ID* cuyo mensaje de error es desplegado sin filtros por el componente cpsrvd, incluso en los puertos de administración de cPanel no expuestos externamente. La configuración por defecto de cPanel permite a través de las reglas de proxy acceder al directorio /cpanelwebcall/, afectando así también a los puertos 80 y 443 del sitio web administrado por cPanel. Esto permitiría a un atacante no autenticado a través de peticiones especialmente diseñadas incluyendo código JavaScript malicioso, ejecutar dicho código en el navegador de la víctima y así potencialmente secuestrar su sesión de cPanel para obtener control del sitio vulnerable.

Impacto:

La explotación exitosa de esta vulnerabilidad podría permitir potencialmente a un atacante no autenticado secuestrar la sesión del usuario de cPanel víctima para obtener control del sitio vulnerable.

Solución:

Recomendamos instalar las actualizaciones correspondientes provistas por el fabricante en el siguiente enlace:

- https://forums.cpanel.net/threads/cpanel-tsr-2023-0001-full-disclosure.708949/

Nota: En caso de que se utilice CPanel como parte de un servicio proporcionado por un proveedor de *hosting*, solicitar o asegurarse que éste lo actualice.

Información adicional:

- https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-29489
- https://forums.cpanel.net/threads/cpanel-tsr-2023-0001-full-disclosure.708949/