BOLETÍN DE ALERTA

Boletín Nro.: 2023-43
Fecha de publicación: 15/09/2023
Tema: Vulnerabilidad de *Cross-Site Scripting (XSS)* en productos Fortinet

Productos afectados:

- FortiProxy, versión 7.2.0 hasta 7.2.4.
- FortiProxy, versión 7.0.0 hasta 7.0.10.
- FortiOS, versión 7.2.0 hasta 7.2.4.
- FortiOS, versión 7.0.0 hasta 7.0.11.
- FortiOS, versión 6.4.0 hasta 6.4.12.
- FortiOS, versión 6.2.0 hasta el 6.2.14.

Descripción:

Se ha reportado un nuevo aviso de seguridad sobre una vulnerabilidad que afecta a FortiOS y FortiProxy de Fortinet, que permitiría a un atacante realizar ataques del tipo *Cross-Site Scripting (XSS*) a través del sitio web afectado.

La vulnerabilidad identificada como CVE-2023-29183, de severidad "Alta", con una puntuación asignada de 8.0. Esta vulnerabilidad del tipo *Cross-Site Scripting (XSS*) se debe a una falla de validación de datos de entrada al generar páginas webs en FortiOS y FortiProxy de Fortinet. Esto permitiría a un atacante autenticado a través de la configuración especialmente diseñada de administración de invitados, realizar ejecución de código JavaScript arbitrario en el navegador de la víctima.

Impacto:

La explotación exitosa de esta vulnerabilidad podría permitir a un atacante realizar ataques del tipo *Cross-Site Scripting (XSS*) a través del sitio web afectado.

Solución:

Recomendamos instalar las actualizaciones correspondientes provistas por el fabricante a través de la siguiente guía:

- https://www.fortiguard.com/psirt/FG-IR-23-106

Información adicional:

- https://www.incibe.es/incibe-cert/alerta-temprana/avisos/cross-site-scripting-en-productos-fortios-y-fortiproxy-de-fortinet
- https://nvd.nist.gov/vuln/detail/CVE-2023-29183
- https://www.fortiguard.com/psirt/FG-IR-23-106