CONCIBER
Comité Nacional de Seguridad Cibernética

ALERTA

Vulnerabilidad de software

Fecha: 14/09/2023

Problemática: Fortinet parchó vulnerabilidades en productos FortiOS, FortiProxy y FortiWeb

Correlativo: AC-0069

Institución / Sector: Instituciones Públicas y Privadas

CONTEXTO

Fortinet lanzó parches para el problema de alta gravedad en la vulnerabilidad identificada como CVE-2023-34984 que afecta al firewall de aplicaciones web y solución de protección API FortiWeb.

SITUACIÓN

La falla presentada provoca la neutralización inadecuada de la entrada durante la generación de la página web del administrador.

La vulnerabilidad afecta a las versiones;

FortiProxy 7.0.x y 7.2.x
FortiOS 6.2.x, 6.4.x, 7.0.x y 7.2.x

Nivel de priorización

Prioridad Urgente / No Urgente	Actualización Seguimiento/Preventiva/Resiliente
Urgente	**Preventiva**

Matriz de Evaluación

Riesgo Alto/ Medio/ Bajo	Nivel de Afectación		
	Integridad	Disponibilidad	Confidencialidad
Alto	**Alto**	**Alta**	**Alta**

RECOMENDACIONES

Ante esta problemática, se recomienda aplicar las actualizaciones para corregir la falla.

Versiones disponibles;

- 7.0.11 y 7.2.5 de FortiProxy.
- 6.2.15, 6.4.13, 7.0.12, 7.2.5 y 7.4.0 de FortiOS

DICCIONARIO DE DATOS

- Atacante (ciberdelincuente, actor de amenazas): Persona que realiza actividades delictivas en la red contra personas o sistemas informáticos, pudiendo provocar daños económicos o reputacionales mediante robo, filtrado de información.
- Vulnerabilidad: Debilidad o fallo de un sistema que puede ser aprovechado con fines maliciosos.

REFERENCIAS

FORTINET
https://www.securityweek.com/fortinet-patches-high-severity-vulnerabilities-in-fortios-fortiproxy-fortiweb-products/?web_view=true