CONCIBER
Comité Nacional de Seguridad Cibernética

ALERTA

Vulnerabilidad en la solución de Ciberseguridad “Fortinet”

Fecha: 16/06/2023

Problemática: Vulnerabilidad de omisión de autenticación remota en firewalls de Fortinet, proxies web

Correlativo: AC-0044

Institución / Sector: Instituciones Públicas y Privadas

CONTEXTO

Fortinet lanzó un comunicado por medio de sus canales oficiales informando a sus consumidores sobre la vulnerabilidad de su software en los productos FortiOS (firewall) y FortiProxy (proxy web). La vulnerabilidad ha sido clasificada como extremadamente crítica y ha sido identificada como “CVE-2022-40684”.

SITUACIÓN

La explotación de esta vulnerabilidad permite a un atacante remoto no autenticado eludir autenticación y obtener acceso a la interfaz administrativa de estos productos con solo una solicitud http/s especialmente diseñada. Las versiones que se ven afectadas por esta vulnerabilidad son:

- FortiOS 7.0.0 a 7.0.6
- FortiOS 7.2.0 a 7.2.1
- FortiProxy 7.0.0 a 7.0.6 y 7.2.0

REFERENCIAS

1. https://docs.fortinet.com/document/fortigate/7.0.7/fortios-release-notes/289806/resolved-issues
2. https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-40684

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	Alta	Alta	Alta

RECOMENDACIONES

Se recomienda encarecidamente a los usuarios de los productos FortiOS y FortiProxy que se ven afectados por esta vulnerabilidad, ejecutar la actualización de la versión del software que corresponda de inmediato, en caso de emergencia.

DICCIONARIO DE DATOS

1. Vulnerabilidad: Debilidad o fallo de un sistema que puede ser aprovechado con fines maliciosos (normalmente mediante un programa que se denomina exploit). Cuando se descubre el desarrollador del software o hardware lo solucionará publicando una actualización de seguridad del producto
2. Ciberdelincuente: Persona que realiza actividades delictivas en la red contra personas o sistemas informáticos, pudiendo provocar daños económicos o reputacionales mediante robo, filtrado de información, deterioro de software o hardware, fraude y extorsión. Casi siempre están orientados a la obtención de fines económicos.
3. CVE: Acrónimo del inglés en Common Vulnerabilities and Exposures; en español, listado de vulnerabilidades de seguridad conocidas, en el que se puede identificar una vulnerabilidad, así como un resumen de las características, efectos, las versiones del software afectadas, posibles soluciones o mitigaciones de dicha vulnerabilidad.