Nro. Alerta:	EC-2022-091	CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS **ALERTA DE SEGURIDAD**	CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS ECUCERT
TLP:	TLP:CLEAR		
Fecha:	12-oct-2022	MÚLTIPLES VULNERABILIDADES EN PRODUCTOS FORTINET	V 1.1

I. DATOS GENERALES:

Clase de alerta: Vulnerabilidad
Tipo de vulnerabilidad: CVE-2022-40684
Nivel de riesgo: Varios niveles de impacto.

II. ALERTA

Múltiples vulnerabilidades en productos Fortinet podrían permitir ataques contra los procesos de autenticación.

Las vulnerabilidades detectadas han sido registradas en los sistemas de métricas de priorización con el registro CVE-2022-40684, que señala como técnicas de ataque utilizadas, peticiones HTTP/HTTPS mediante paquetes de datos personalizados.

Figura No. 1: Vulnerabilidades Fortinent

III. INTRODUCCIÓN

Fortinet es una empresa que provee soluciones de ciberseguridad. FortiProxy es un proxy seguro que protege a los usuarios en contra de ataques realizados a través de Internet mediante tecnicass de detección. FortiSwitch Manager es una plataforma in situ la cual gestiona a la herramienta FortiSwitch. Una vulnerabilidad ha sido descubierta en el sistema operativo FortiOS, y las herramientas de FortyProxy que permitiría la realización de ataques en contra de los procesos de autenticación a estos sistemas.

Dirección: Av. 9 de Octubre N27-75 y Berlín
Código Postal: 170513 / Quito - Ecuador
Teléfono: 593-2 2946 400 - www.arcotel.gob.ec

Nro. Alerta:	EC-2022-091	CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS **ALERTA DE SEGURIDAD**	CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS ECUCERT
TLP:	TLP:CLEAR		
Fecha:	12-oct-2022	MÚLTIPLES VULNERABILIDADES EN PRODUCTOS FORTINET	V 1.1

Las vulnerabilidades detectadas afectan a las versiones:

- FortiOS version 7.2.0 through 7.2.1
- FortiOS version 7.0.0 through 7.0.6
- FortiProxy version 7.2.0
- FortiProxy version 7.0.0 through 7.0.6
- FortiSwitchManager version 7.2.0
- FortiSwitchManager version 7.0.0

IV. VECTOR DE ATAQUE:

Peticiones HTTP/HTTPS mediante paquetes maliciosos. Las interfaces para administración de los sistemas vulnerables son el módulo explotado con los paquetes maliciosos creados por los atacantes.

V. IMPACTO:

En consideración al tipo de arquitectura y alcance de la red en la que se encuentre se han definido los siguientes tipos de impacto:

- Redes Institucionales de gran alcance: Alto
- Redes Institucionales de bajo alcance: Alto
- Redes de Hogar: Bajo

VI. INDICADORES DE COMPROMISO:

No aplica.

VII. RECOMENDACIONES:

El Centro de Respuestas a Incidentes Informáticos de ARCOTEL, EcuCERT, recomienda a su comunidad objetivo y a la ciudadanía lo siguiente:

- Aplicar los parches de seguridad y procedimientos mitigatorios definidos por el desarrollador de la aplicación.
- Verificar el proceso de actualización automática de la herramienta.
- Verificar el principio de menor privilegio respecto de la gestión de cuentas de usuarios.
- Restringir el acceso y uso de ciertas páginas web, bloquear actividades de descarga de adjuntos, bloquear scripts automáticos java y extensión de navegadores.

Dirección: Av. 9 de Octubre N27-75 y Berlín
Código Postal: 170513 / Quito - Ecuador
Teléfono: 593-2 2946 400 - www.arcotel.gob.ec

Nro. Alerta:	EC-2022-091	CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS **ALERTA DE SEGURIDAD**	CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS ECUCERT
TLP:	TLP:CLEAR		
Fecha:	12-oct-2022	MÚLTIPLES VULNERABILIDADES EN PRODUCTOS FORTINET	V 1.1

- Informar y educar a usuarios en relación a las amenazas generadas por enlaces contenidos en correos electrónicos y mensajes sms, de manera especial los provenientes de fuentes no conocidas.

VIII. DESCARGO DE RESPONSABILIDAD

- La información en esta alerta es con fines informativos. El Centro de Respuestas de ARCOTEL, EcuCERT, no respalda ningún producto o servicio comercial, incluidos aquellos sujetos de análisis.
- Cualquier referencia a productos, procesos o servicios comerciales específicos por marca de servicio, marca comercial, fabricante, no constituye ni implica respaldo, recomendación o favorecimiento por parte de EcuCERT.
- La presente alerta no debe utilizarse con fines publicitarios o de patrocinio de productos.

IX. REFERENCIAS:

- *FortiGuard Labs. (2022, 10 octubre). FortiOS / FortiProxy / FortiSwitchManager - Authentication bypass on administrative interface Recuperado de https://www.fortiguard.com/psirt/FG-IR-22-377.*
- *MITRE. (2022). CVE-2022-40684. Recuperado de https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-40684*
- *Gatlan, S. (2022, 7 octubre). Fortinet warns admins to patch critical bypass bug inmediately Recuperado de https://www.bleepingcomputer.com/news/security/fortinet-warns-admins-to-patch-critical-auth-bypass-bug-immediately/*