
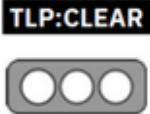


Nro. Alerta:	AL-2023-014	CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS DEL ECUADOR	
TLP:			
Fecha:	20-mar-2023	<b>Nueva vulnerabilidad identificada de FortiOS permite ejecutar código arbitrario</b>	

**I. DATOS GENERALES:**

**Clase de alerta:** Vulnerabilidad  
**Tipo de incidente:** Explotación de vulneraciones conocidas  
**Nivel de riesgo:** Alto

**II. ALERTA**


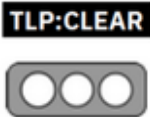


**Figura 1.-** Fortinet: nuevo error de FortiOS utilizado como día cero para atacar redes gubernamentales  
**Fuente:** BleepingComputer

Fortinet lanzó actualizaciones de seguridad el 7 de marzo de 2023 para abordar una vulnerabilidad de seguridad con puntaje de gravedad alto (CVE-2022-41328) que permite a los actores de amenazas ejecutar códigos o comandos no autorizados.

**III. INTRODUCCIÓN**

Los actores de amenazas explotan la vulnerabilidad FG-IR-22-369 / CVE-2022-41328; esta falla permite ejecutar código arbitrario y ya ha causado pérdida de datos y corrupción del sistema en organizaciones objetivo. La vulnerabilidad afecta a varias versiones de FortiOS.

Nro. Alerta:	AL-2023-014	CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS DEL ECUADOR	
TLP:			
Fecha:	20-mar-2023	<b>Nueva vulnerabilidad identificada de FortiOS permite ejecutar código arbitrario</b>	

El incidente se descubrió después de que los dispositivos Fortigate comprometidos se apagaran con los mensajes “System enters error-mode due to FIPS error: Firmware Integrity self-test failed”.

Fortinet ha indicado que esto sucede porque sus dispositivos habilitados para FIPS verifican la integridad de los componentes del sistema y están configurados para apagarse automáticamente y detener el arranque para bloquear una brecha en la red si se detecta un compromiso.

#### IV. VECTOR DE ATAQUE:

El equipo de investigación de Fortinet, descubrió que dentro de la imagen del firmware de un dispositivo comprometido, **/sbin/init**, se había modificado y se había agregado un nuevo archivo, **/bin/fgfm**. La modificación de **/sbin/init** garantiza que **/bin/fgfm**, pueda proporcionar a un atacante acceso y control persistente y que el archivo se ejecute antes de continuar con las acciones de arranque habituales.


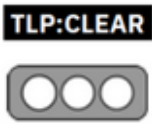
#### V. IMPACTO:

CVE-2022-41328 es una vulnerabilidad de cruce de ruta que surge de un error de autenticación al procesar un comando CLI específico y afecta a las siguientes versiones de FortiOS:

- FortiOS versión 7.2.0 a 7.2.3
- FortiOS versión 7.0.0 a 7.0.9
- FortiOS versión 6.4.0 a 6.4.11
- FortiOS 6.2 todas las versiones
- FortiOS 6.0 todas las versiones

Las actualizaciones que abordan la vulnerabilidad están disponibles en versiones;

- Actualice a FortiOS versión 7.2.4 o superior
- Actualice a FortiOS versión 7.0.10 o superior
- Actualice a FortiOS versión 6.4.12 o superior

Nro. Alerta:	AL-2023-014	CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS DEL ECUADOR  <b>ALERTAS DE SEGURIDAD</b>	 V 1.1
TLP:			
Fecha:	20-mar-2023	<b>Nueva vulnerabilidad identificada de FortiOS permite ejecutar código arbitrario</b>	Pág.: 3 of 3

## VI. RECOMENDACIONES:

El EcuCERT recomienda a su comunidad objetivo tomar en consideración lo siguiente:

- Actualizar el sistema operativo FortiOS a la última versión liberada por el fabricante.
- Realizar evaluaciones de seguridad periódicas y los escaneos de vulnerabilidades en la red a fin de identificar y abordar posibles problemas de seguridad antes de que los actores malintencionados los exploten.
- Mantener monitoreo de la Red para identificar cualquier comportamiento anómalo.

## VII. REFERENCIAS:

Brandefense. (16 de 03 de 2023). *Brandefense*. Obtenido de <https://brandefense.io/security-news/fortios-vulnerability-exploitation/>

*Fortiguard Labs*. (s.f.). Obtenido de [https://www.fortinet.com/blog/psirt-blogs/fg-ir-22-369-psirt-analysis?utm\\_source=brandefense&utm\\_medium=secnews](https://www.fortinet.com/blog/psirt-blogs/fg-ir-22-369-psirt-analysis?utm_source=brandefense&utm_medium=secnews)

Fortinet. (s.f.). *Análisis de FG-IR-22-369*. Obtenido de [https://www.fortinet.com/blog/psirt-blogs/fg-ir-22-369-psirt-analysis?utm\\_source=brandefense&utm\\_medium=secnews](https://www.fortinet.com/blog/psirt-blogs/fg-ir-22-369-psirt-analysis?utm_source=brandefense&utm_medium=secnews)

Fortinet. (s.f.). *Fortiguard - Fortinet*. Obtenido de <https://www.fortiguard.com/psirt/FG-IR-22-369>

Gatlán, S. (13 de mar de 2023). *BleepingComputer*. Obtenido de <https://www.bleepingcomputer.com/news/security/fortinet-new-fortios-bug-used-as-zero-day-to-attack-govt-networks/>

*NIST*. (s.f.). Obtenido de <https://nvd.nist.gov/vuln/detail/CVE-2022-41328>