Nro. Alerta:	AL-2024-022	CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS DEL ECUADOR ALERTAS DE SEGURIDAD	ecucert V 1.2
TLP:	TLP:CLEAR		
Fecha:	25-oct-2024	VULNERABILIDAD EN FORTIMANAGER	Pág.: **1** of **6**

I. DATOS GENERALES:

Clase de alerta: Vulnerabilidad
Tipo de incidente: Información
Nivel de riesgo: Alto

II. ALERTA

Fortinet ha hecho pública una vulnerabilidad crítica denominada 'FortiJump', que afecta al producto FortiManager. La explotación de esta vulnerabilidad podría permitir a un atacante, remoto y no autenticado, ejecutar código.

Figura 1.- *Ilustración asociada a Fortinet.* ***Fuente:*** *Cyber Security News*

III. INTRODUCCIÓN

El 23 de octubre de 2024, Fortinet publicó un aviso de seguridad con el CVE-2024-47575, que corresponde una vulnerabilidad crítica de día cero que afecta a su solución de gestión de redes FortiManager. La vulnerabilidad surge de una falta de autenticación para una función crítica [CWE-306] en el demonio fgfmd de FortiManager que permite a un atacante remoto no autenticado ejecutar código o comandos

arbitrarios a través de solicitudes especialmente diseñadas. La vulnerabilidad tiene una puntuación CVSS v3 de 9,8.

IV. VECTOR DE ATAQUE:

Las siguientes versiones del producto FortiManager se ven afectadas:

- Versiones de FortiManager 7.6 anteriores a 7.6.1;
- Versiones de FortiManager 7.4 anteriores a 7.4.5;
- Versiones de FortiManager 7.2 anteriores a 7.2.8;
- Versiones de FortiManager 7.0 anteriores a 7.0.13;
- Versiones de FortiManager 6.4 anteriores a 6.4.15;
- Versiones de FortiManager 6.2 anteriores a 6.2.13;
- Versiones de FortiManager Cloud 7.4 anteriores a 7.4.5;
- FortiManager Cloud 7.2 todas las versiones;
- FortiManager Cloud 7.0 todas las versiones;
- FortiManager Cloud 6.4 todas las versiones;

V. INDICADORES DE COMPROMISO

Los siguientes indicadores se pueden utilizar para identificar un riesgo potencia, pero no aparecer en todos los casos.

- LOGs y palabras claves

  type=event,subtype=dvm,pri=information,desc="Device,manager,generic,information,log",user="device,...",msg="Unregistered device localhost add succeeded" device="localhost" adom="FortiManager" session_id=0 operation="Add device" performed_on="localhost" changes="Unregistered device localhost add succeeded"

  type=event,subtype=dvm,pri=notice,desc="Device,Manager,dvm,log,at,notice,level",user="System",userfrom="",msg="" adom="root" session_id=0 operation="Modify device" performed_on="localhost" changes="Edited device settings (SN FMG-VMTM23017412 ó FMG-VMTM19008093)"

- IPs
  45.32.41.202
  104.238.141.143
  158.247.199.37
  45.32.63.2
  195.85.114.78
  80.66.196.199
  198.199.122.22
  172.232.167.68

- Archivos
  /tmp/.tm
  /var/tmp/.tm
  Hash MD5: 9DCFAB171580B52DEAE8703157012674

VI. IMPACTO:

Ejecución de código o comandos no autorizados. Las acciones identificadas de este ataque han sido las de automatizar mediante scripts la exfiltración de archivos del FortiManager que contenían las IP, credenciales y configuraciones de los dispositivos gestionados.

No se tiene informes de ninguna instalación de malware o puertas traseras de bajo nivel en los sistemas FortiManager comprometidos. Aún, no ha existido indicios de bases de datos modificadas, ni conexiones y modificaciones en los dispositivos administrados.

VII. RECOMENDACIONES:

- Actualizar los dispositivos afectados lo antes posible, priorizando los activos conectados a Internet. Cuando no sea posible, se recomienda aplicar una solución alternativa.

Versión	Afectado	Solución
FortiManager 7.6	7.6.0	Actualizar a 7.6.1 o superior
FortiManager 7.4	7.4.0 a 7.4.4	Actualizar a 7.4.5 o superior
FortiManager 7.2	7.2.0 a 7.2.7	Actualizar a 7.2.8 o superior
FortiManager 7.0	7.0.0 a 7.0.12	Actualizar a 7.0.13 o superior
FortiManager 6.4	6.4.0 a 6.4.14	Actualizar a 6.4.15 o superior
FortiManager 6.2	6.2.0 a 6.2.12	Actualizar a 6.2.13 o superior
Nube FortiManager 7.6	No afectado	No aplicable
Nube FortiManager 7.4	7.4.1 a 7.4.4	Actualizar a 7.4.5 o superior
Nube FortiManager 7.2	7.2.1 a 7.2.7	Actualizar a 7.2.8 o superior
Nube FortiManager 7.0	7.0.1 a 7.0.12	Actualizar a 7.0.13 o superior
Nube FortiManager 6.4	6.4 todas las versiones	Migrar a una versión no vulnerable

Soluciones alternativas

1. Para las versiones de FortiManager 7.0.12 o superior, 7.2.5 o superior, 7.4.3 o superior (pero no 7.6.0), evitar que dispositivos desconocidos intenten registrarse.

```
config system global
(global)# set fgfm-deny-unknown enable
(global)# end
```

Si las actualizaciones de FortiGate o el filtrado web están habilitados, bloquear la adición de dispositivos no autorizados a través de FDS.

```
conf fmupdate fds-setting
set unreg-dev-option ignore
end
```

2. Como alternativa, para las versiones 7.2.0 y superiores de FortiManager, se puede agregar políticas locales para incluir en la lista blanca las direcciones IP de FortiGates que tienen permitido conectarse.

3. Para 7.2.2 y superiores, 7.4.0 y superiores, 7.6.0 y superiores utilizar un certificado personalizado.

```
config system global
set fgfm-ca-cert
set fgfm-cert-exclusive enable
end
```

- Cambiar las credenciales, incluidas las contraseñas y los datos confidenciales del usuario, de todos los dispositivos administrados conectados a los sistemas FortiManager afectados.

VIII. DESCARGO DE RESPONSABILIDAD

- La información en la presente alerta, se proporciona con fines informativos.
- Cualquier referencia a productos, procesos o servicios comerciales específicos, no constituye respaldo o recomendación por parte del EcuCERT a los mismos.
- La presente alerta no debe utilizarse con fines publicitarios o de patrocinio de productos.

IX. REFERENCIAS:

- https://cert.europa.eu/publications/security-advisories/2024-113/
- https://cloud.google.com/blog/topics/threat-intelligence/fortimanager-zero-day-exploitation-cve-2024-47575
- https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2024-47575
- https://cybersecuritynews.com/fortimanager-devices-mass-compromise/
- https://nvd.nist.gov/vuln/detail/CVE-2024-47575

- https://www.fortiguard.com/psirt/FG-IR-24-423
- https://www.incibe.es/incibe-cert/alerta-temprana/avisos/vulnerabilidad-0day-de-ejecucion-de-codigo-remoto-en-fortimanager-de-fortinet
- https://www.rapid7.com/blog/post/2024/10/23/etr-fortinet-fortimanager-cve-2024-47575-exploited-in-zero-day-attacks/

Nota (línea de tiempo):

- **2024-11-12:** Actualización de indicadores de compromiso