Nro. Alerta:	AL-2025-015	CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS DEL ECUADOR	ecucert
TLP:	TLP:CLEAR	**ALERTAS DE SEGURIDAD**	V 1.1
Fecha:	10-abr-2025	FortiSwitch (CVE-2024-48887)	Pág.: **1** of **3**

I. DATOS GENERALES:

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

II. ALERTA

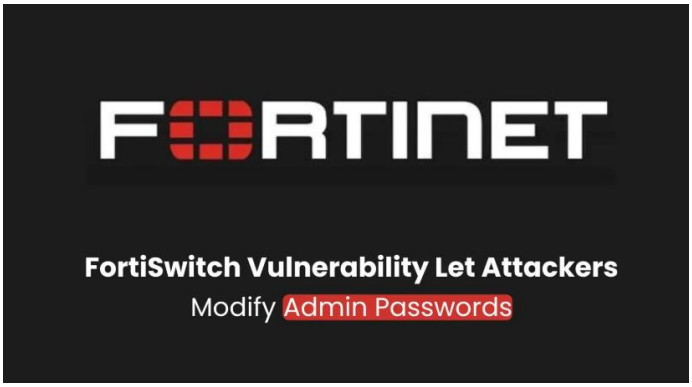

Figura 1.- FortiSwitch - figura referencial

CVE-2024-48887, es una vulnerabilidad de cambio de contraseña no verificada en la Fortinet FortiSwitch GUI, la cual puede permitir que un atacante remoto no autenticado cambie las contraseñas de administrador a través de una solicitud especialmente manipulada.

III. INTRODUCCIÓN

FortiSwitch es un switch de red que ofrece seguridad, rendimiento y administración de redes, entre sus características están: protege contra amenazas de loT, permite controlar dispositivos de red de terceros, orquesta una respuesta automática a eventos de red, se integra con la plataforma FortiGate (firewall de próxima generación -NGFW- que protege redes contra amenazas cibernéticas), permite la centralización de la administración de la red y ofrece conectividad confiable para loT, OT y redes industriales.

Esta vulnerabilidad identificada como "fallo de cambio de contraseña no verificada" (CWE-620), podría permitir a atacantes remotos no autenticados modificar contraseñas administrativas mediante solicitudes manipuladas por medio de la interfaz gráfica de usuario (GUI) de FortiSwitch.

IV. VECTOR DE ATAQUE

El ataque se lleva a cabo de manera remota y es del tipo network CVSS:3.1/AV:**N**/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

V. IMPACTO

Esta vulnerabilidad tiene un impacto de escalamiento de privilegio y afecta a las versiones:

Versión	Afectación
FortiSwitch 7.6	V 7.6.0
FortiSwitch 7.4	De 7.4.0 hasta 7.4.4
FortiSwitch 7.2	De 7.2.0 hasta 7.2.8
FortiSwitch 7.0	De 7.0.0 hasta 7.0.10
FortiSwitch 6.4	De 6.4.0 hasta 6.4.14

Tabla 1.- Versiones afectadas FortiSwitch

VI. RECOMENDACIONES:

Fortinet recomienda actualizar a las versiones:

- De 7.6 a versiones 7.6.1 o superior.
- De 7.4 a versiones 7.4.5 o superior.
- De 7.2 a versiones 7.2.9 o superior.
- De 7.0 a versiones 7.0.11 o superior.
- De 6.4 a versiones 6.4.15 o superior.
- En caso de no poder actualizar inmediatamente se sugiere: restablecer el acceso a las interfaces administrativas deshabilitando los servicios HTTP/HTTPS.
- Limitar las conexiones a los hosts de confianza sólo usando los siguientes comandos.

```
config system admin
edit
set {trusthost1 | trusthost2 | trusthost3}
next
end
```

VII. 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.

VIII. REFERENCIAS:

https://www.cvedetails.com/cve/CVE-2024-48887/

https://www.cve.org/CVERecord?id=CVE-2024-48887

https://cybersecuritynews.com/fortinet-warns-of-fortiswitch-vulnerability/

https://fortiguard.fortinet.com/psirt/FG-IR-24-435

https://nvd.nist.gov/vuln/detail/CVE-2024-48887

https://devel.group/blog/una-falla-critica-pone-en-riesgo-la-seguridad-de-fortiswitch/