Nro. Alerta:	AL-2025-003	CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS DEL ECUADOR **ALERTAS DE SEGURIDAD**	ecucert V 1.1
TLP:	TLP:CLEAR		
Fecha:	20-ene-2025	**Vulnerabilidad en Firewall FORTINET**	Pág.: **1** of **8**

I. DATOS GENERALES:

Clase de alerta: Vulnerabilidad

Tipo de vulnerabilidad: Vulnerabilidad (CVE-2024-55591) en firewalls Fortinet FortiOS y FortiProxy

Nivel de riesgo: Alta

II. ALERTA

Figura 1.- *F*irewalls Fortinet FortiOS y FortiProxy – vulnerabilidad (CVE-2024-55591)

CVSS:

Score	Severity	Version	Vector String
9.6	CRITICAL	3.1	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H/E:H/RL:W/RC:C

Figura 2.- CVSS - ***F***firewalls Fortinet FortiOS y FortiProxy – vulnerabilidad (CVE-2024-55591)

III. INTRODUCCIÓN

FORTINET ha publicado respecto a una vulnerabilidad de omisión de autenticación mediante una ruta o canal alternativo [CWE-288] que afecta a FortiOS versión 7.0.0 a 7.0.16 y FortiProxy versión 7.0.0 a 7.0.19 y 7.2.0 a 7.2.12, permite a un atacante remoto obtener privilegios de superadministrador a través de solicitudes diseñadas al módulo websocket Node.js.

CVE-2024-55591 es una vulnerabilidad crítica de omisión de autenticación que explota rutas o canales alternativos. Los atacantes pueden obtener privilegios de superadministrador mediante solicitudes diseñadas al módulo WebSocket de Node.js, lo que permite la ejecución no autorizada de código o comandos.

IV. VECTOR DE ATAQUE:

Los informes muestran que esto se está explotando de forma generalizada.

CVE	Versión	Afectado	Solución
CVE-2024-55591	FortiOS 7.0	7.0.0 a 7.0.16	Actualización a 7.0.17 o superior
	FortiProxy 7.2	7.2.0 a 7.2.12	Actualización a 7.2.13 o superior
	FortiProxy 7.0	7.0.0 a 7.0.19	Actualización a 7.0.20 o superior

Tabla 1.- Firewalls Fortinet FortiOS y FortiProxy – vulnerabilidad (CVE-2024-55591)

La vulnerabilidad, que está siendo explotada en la actualidad, ha sido parcheada por FORTINET, al tiempo que se han publicado Indicadores de Compromiso (IOC).

Tácticas, Técnicas, y Procedimientos (TTPs)		
Táctica	**Técnica**	**Sub-técnicas o Herramientas**
Acceso inicial	T1190: Explotar aplicación Pública	Explotó las interfaces de administración del firewall FortiGate de cara al público
Persistencia	T1136.001: Crear cuenta: Cuenta local	Creación de múltiples cuentas de administrador local
	T1133: Servicios remotos externos	Modificación de configuraciones de VPN SSL
	T1078.001: Cuentas válidas: Cuentas predeterminadas	Secuestración de una cuenta de invitado predeterminada para obtener acceso a VPN SSL
Acceso a Credenciales	T1003.006: Volcado de credenciales del SO: DCSync	Los actores de amenazas utilizaron una cuenta de administrador de dominio para llevar a cabo un ataque DCSync

Tabla 2.- Tácticas, Técnicas, y Procedimientos - Firewalls Fortinet FortiOS y FortiProxy – vulnerabilidad (CVE-2024-55591)

V. IMPACTO:

Fortinet ha solucionado una vulnerabilidad de omisión de autenticación (CVE-2024-55591) en sus firewalls FortiOS y gateways web FortiProxy. Los atacantes han explotado activamente esta falla como vulnerabilidad de día cero para comprometer los firewalls FortiGate expuestos públicamente.

FORTINET en su aviso de seguridad, confirmó la explotación in situ de la vulnerabilidad, compartió información mínima relacionada con el ataque y algunos indicadores de compromiso (IoC). Estos IoC incluyen:

- Direcciones IP
- Entradas de registro
- Usuarios creados
- Una lista de operaciones realizadas por los atacantes

Algunos de estos IoC se superponen con los hallazgos de los investigadores de Arctic Wolf. Su análisis detalla una campaña de ataque que comenzó a mediados de noviembre, que incluyó inicios de sesión administrativos no autorizados, creación de nuevas cuentas, autenticación SSL VPN y varios cambios de configuración.

VI. INDICADORES DE COMPROMISO

Las siguientes entradas de registro son posibles IOC:

- Siguiente registro de actividad de inicio de sesión con script y dstip aleatorios:

  ✓ type="event" subtype="system" level="information" vd="root" logdesc="Admin login successful" sn="1733486785"
  ✓ user="admin" ui="jsconsole" method="jsconsole" srcip=1.1.1.1 dstip=1.1.1.1 action="login" status="success"
  ✓ reason="none" profile="super_admin" msg="Administrator admin logged in successfully from jsconsole"

- Siguiente registro de creación de administrador con nombre de usuario y dirección IP de origen aparentemente generados aleatoriamente:

  ✓ type="event" subtype="system" level="information" vd="root" logdesc="Object attribute configure" user="admin"
  ✓ ui="jsconsole(127.0.0.1)" action="Add" cfgtid=1411317760 cfgpath="system.admin" cfgobj="vOcep"
  ✓ cfgattr="password[*]accprofile[super_admin]vdom[root]" msg="Add system.admin vOcep"

- En los registros anteriores, los atacantes encontraron principalmente las siguientes direcciones IP:

  ✓ 1.1.1.1
  ✓ 127.0.0.1
  ✓ 2.2.2.2
  ✓ 8.8.8.8
  ✓ 8.8.4.4

Se debe considerar:

- Tenga en cuenta que los parámetros IP anteriores no son las direcciones IP de origen reales del tráfico de ataque, sino que los genera arbitrariamente el atacante como parámetro. Por este motivo, no se deben utilizar para ningún bloqueo.

- Tenga en cuenta también que sn y cfgtid no son relevantes para el ataque.

- Las operaciones realizadas por el actor de amenazas (TA) en los casos que observamos fueron parte o la totalidad de las siguientes:

  ✓ Creación de una cuenta de administrador en el dispositivo con un nombre de usuario aleatorio
  ✓ Creación de una cuenta de usuario local en el dispositivo con un nombre de usuario aleatorio

- ✓ Creación de un grupo de usuarios o adición del usuario local anterior a un grupo de usuarios de sslvpn existente
- ✓ Adición o modificación de otras configuraciones (política de firewall, dirección de firewall, ...)
- ✓ Inicio de sesión en sslvpn con los usuarios locales agregados anteriormente para obtener un túnel a la red interna.

- El usuario administrador o local creado por el TA se genera aleatoriamente. p. ej.:

  - ✓ Gujhmk
  - ✓ Ed8x4k
  - ✓ G0xgey
  - ✓ Pvnw81
  - ✓ Alg7c4
  - ✓ Ypda8a
  - ✓ Kmi8p4
  - ✓ 1a2n6t
  - ✓ 8ah1t6
  - ✓ M4ix9f

- Además, se ha visto que el TA utiliza las siguientes direcciones IP:

  - ✓ 45.55.158.47 [dirección IP más utilizada]
  - ✓ 87.249.138.47
  - ✓ 155.133.4.175
  - ✓ 37.19.196.65
  - ✓ 149.22.94.37

VII. RECOMENDACIONES:

- **Actualice** a una versión fija: FortiOS 7.0.17 o posterior, FortiProxy 7.2.13 o posterior, o 7.0.20 o posterior

- Si no es posible realizar actualizaciones inmediatas, **implemente soluciones alternativas**, como eliminar la interfaz de administración basada en web del firewall de Internet público

- **Restringir la exposición de la interfaz de administración:** las interfaces de administración nunca deben ser accesibles públicamente. Limitar el acceso a usuarios internos de confianza.

- **Monitorear la actividad sospechosa:** estar atento a actividad de jsconsole desde direcciones IP falsificadasTráfico de administración web de más de 1 MB en la interfaz WAN que se origina en proveedores de alojamiento VPSInicios de sesión inesperados desde direcciones IP de proveedores de alojamiento VPS

- **Deshabilitar la interfaz administrativa** HTTP/HTTPS

- **Limite las direcciones IP** que pueden acceder a la interfaz administrativa mediante políticas de entrada local:

```
configure la dirección del firewall
edit "my_allowed_addresses"
set subnet
end
```

- Luego, **crea un grupo de direcciones**:

```
config firewall addrgrp
edit "MGMT_IPs"
set member "my_allowed_addresses"
end
```

- **Cree la política local** para restringir el acceso solo al grupo predefinido en la interfaz de administración (aquí: port1):

```
config firewall local-in-policy
edit 1
set intf port1
set srcaddr "MGMT_IPs"
set dstaddr "all"
set action accept
set service HTTPS HTTP
```

```
set schedule "always"
set status enable
next

edit 2
set intf "all"
set srcaddr "all"
set dstaddr "all"
set action deny
set service HTTPS HTTP
set schedule "always"
set status enable
end
```

- Si utiliza puertos que no son los predeterminados, **cree un objeto de servicio adecuado** para el acceso administrativo de la GUI:

```
config firewall service custom
edit GUI_HTTPS
set tcp-portrange 443
next

edit GUI_HTTP
set tcp-portrange 80
end
```

- **Utilice estos objetos en lugar de "HTTPS HTTP"** en las políticas de entrada local 1 y 2 que se indicaron.

- **Tenga en cuenta que la función trusthost logra lo mismo que las políticas de entrada** local anteriores solo si todos los usuarios de la GUI están configurados con ella. Por lo tanto, las políticas de entrada local anteriores son la solución alternativa preferida.

- **Tenga en cuenta también que un atacante necesita saber el nombre de usuario de una cuenta de administrador para realizar el ataque e iniciar sesión en la CLI.** Por lo tanto, tener un nombre de usuario no estándar y que no se pueda adivinar para las cuentas de administrador ofrece cierta protección y, en general, es una buena práctica. Sin embargo, tenga en cuenta que, dado que el websocket de

destino no es un punto de autenticación, nada evitaría que un atacante use la fuerza bruta para obtener el nombre de usuario.

- **Comuníquese con el servicio de atención al cliente** de FORTINET para obtener ayuda.

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:

- **FortiGuard Labs (2024).** *Authentication bypass in Node.js websocket module* https://fortiguard.fortinet.com/psirt/FG-IR-24-535
- **CCN-CERT (2024*).*** *CCN-CERT AL 03/25 Vulnerabilidad crítica en FortiOS y FortiProxy* https://www.ccn-cert.cni.es/es/seguridad-al-dia/alertas-ccn-cert/13042-ccn-cert-al-03-25-vulnerabilidad-critica-en-fortios-y-fortiproxy.html
- **CVE (2024*).*** *CVE-2024-55591* ***https://www.cve.org/CVERecord?id=CVE-2024-55591***