

Exposición de Servicio de Transcripción (Gemini) sin Autenticación

Severidad

Crítica – El endpoint permite uso ilimitado de un servicio externo de pago y expone recursos internos sin control alguno.

el endpoint `/transcribe` acepta archivos de audio y devuelve una transcripción generada mediante un modelo externo (Gemini).

El análisis revela que **no se requiere autenticación, no se limita el tamaño del archivo y no se controla la frecuencia de las solicitudes**, lo que permite el uso ilimitado del servicio por cualquier tercero.

En la práctica, el servidor funciona como un **proxy público hacia Gemini**, exponiendo la clave del proveedor indirectamente y permitiendo su uso sin restricciones.

Impacto

- **Robo de recursos del proveedor (Gemini):**

Atacantes pueden usar el modelo de IA a coste del propietario del servidor.

- **Riesgo económico:**

Generación de facturas elevadas por uso no autorizado de la API de IA.

- **Abuso del servicio:**

Cualquier persona puede usar el endpoint para transcribir audios privados, comerciales o automatizados.

- **Negación de servicio (DoS):**

Envío de audios muy pesados o flood de peticiones puede saturar:

- CPU
- RAM
- cuota de transcripciones del proveedor

- **Exposición indirecta de la clave de IA:**

Aunque la key no se filtra en la respuesta, su uso libre permite inferir que existe una **configuración insegura del backend**.

Evidencia Sanitizada

El auditor pudo ejecutar:

```
curl -X POST "https://api.senaticmia.com/transcribe" \  
-H "accept: application/json" \  
-F "audio_file=@prueba_raw.wav;type=audio/wav"
```

```
{"status":200,"message":"Audio transcribed successfully","content":"probando una prueba para senatic. Uno dos.\n"}
```

Esto confirma que el servicio es completamente público.

Recomendación

- **Requerir autenticación obligatoria** (JWT / API Key) para acceder a [/transcribe](#).
- **Aplicar rate limiting** para evitar abuso y DoS.
- **Limitar tamaños de archivo** (por ejemplo < 10 MB).
- **Validar tipo MIME del archivo** para evitar cargas indebidas.
- **Registrar cada uso** en logs internos para detectar abuso.