Cert-IX

SERVIDOR MCP · SEGURIDAD DE DEPENDENCIAS

DepCheck MCP

Guía del usuario

Todo lo que necesitas para conectar DepCheck a tu agente de programación con IA y comprobar las dependencias en busca de vulnerabilidades conocidas antes de que lleguen a tu código.

Herramienta gratuita para desarrolladores · Model Context Protocol

ENDPOINT:
`https://mcp.cert-ix.com/depcheck`

Contenido

1 Descripción general

Todo lo que necesitas para conectar DepCheck a tu agente de programación con IA y comprobar las dependencias en busca de vulnerabilidades conocidas antes de que lleguen a tu código.

- **Endpoint:** `https://mcp.cert-ix.com/depcheck`
- **Transport:** streamable HTTP (MCP)
- **OSV · CISA KEV · EPSS**

2 Conecta tu agente

Primero, solicita una clave gratuita en cert-ix.com/contact: te enviamos una clave con el formato cixmcp_… (no hace falta cuenta). Después, apunta tu agente al endpoint con esa clave.

Claude Code

```
claude mcp add --transport http depcheck https://mcp.cert-ix.com/depcheck \
  --header "Authorization: Bearer <your-key>"
```

Cualquier cliente MCP (archivo de configuración)

```
{
  "mcpServers": {
    "depcheck": {
      "type": "http",
      "url": "https://mcp.cert-ix.com/depcheck",
      "headers": { "Authorization": "Bearer <your-key>" }
    }
  }
}
```

> Funciona con Claude Code y cualquier cliente que hable MCP sobre HTTP. Una vez que tu clave esté activa, tu agente podrá invocar las herramientas de inmediato.

3 Las cinco herramientas

`check_package`

Argumentos: `ecosystem` `name` `version`

Comprueba la versión de un paquete en busca de vulnerabilidades conocidas. Devuelve los avisos que afectan exactamente a esa versión y la versión segura más cercana a la que actualizar.

`scan_dependencies`

Argumentos: `manifest_content` `manifest_name`

Analiza un manifiesto completo de una vez: go.mod, package.json, package-lock.json, requirements.txt, pyproject.toml, Cargo.toml, Cargo.lock, pom.xml, composer.json. El servidor alojado recibe el cuerpo del archivo, nunca una ruta. Hasta 2000 dependencias por análisis.

`suggest_safe_version`

Argumentos: `ecosystem` `name`

Obtén la versión más reciente de un paquete que no tenga ningún aviso conocido.

`get_advisory`

Argumentos: `id`

Consulta todo el detalle de cualquier aviso (GHSA-…, CVE-…, RUSTSEC-…, GO-…): descripción, CVSS, rangos afectados y referencias.

`get_cve_intel`

Argumentos: `id`

Consulta la inteligencia de explotación de un CVE (estado en CISA KEV y puntuación EPSS) para decidir qué corregir primero. Un problema en la lista KEV o con EPSS alto se está explotando activamente y debería adelantarse en la cola.

4 Cómo leer un veredicto

Campo	Significado
`verdict`	VULNERABLE u OK para la versión exacta comprobada.
`advisories`	Cada uno con un id, una gravedad y una puntuación CVSS.
`exploitation`	Se marca cuando el problema está en CISA KEV o tiene un EPSS alto: corrige estos primero.
`recommended_min_version`	La versión más cercana por encima de la actual que resuelve los avisos.

5 Cómo se tratan tus datos

- No se almacena nada. Tu manifiesto se analiza en memoria para extraer los nombres y las versiones de los paquetes, y luego se descarta: no conservamos ni tus archivos ni tus resultados.
- Solo se comprueban las coordenadas: el nombre y la versión del paquete, nunca el contenido de tus archivos. Las consultas se guardan brevemente en caché en memoria por rapidez.
- Espejo soberano primero. Las comprobaciones se ejecutan contra nuestro propio espejo de avisos alojado en infraestructura de la EU, de modo que la mayoría de las consultas nunca salen de Cert-IX.

> Egreso de respaldo: cuando el espejo no puede responder con certeza sobre un paquete, el nombre y la versión de ese paquete se consultan en la API pública de OSV.dev (operada por OpenSSF). Así que las coordenadas del paquete, no el contenido de los archivos, pueden salir de nuestra infraestructura por esa vía. Tenlo en cuenta si compruebas nombres de paquetes privados o internos.

6 Uso razonable y límites

- Las solicitudes tienen un límite de tasa por clave (aproximadamente 20 por segundo). El análisis de un manifiesto completo es una única solicitud.
- Mantén tu clave en privado: una clave por equipo o usuario. Para rotarla, solicita una nueva y retiramos la antigua.

7 Resolución de problemas

Respuesta	Qué significa
`401 unauthorized`	Clave ausente o no válida: revisa tu cabecera Authorization: Bearer.
`429 too many requests`	Alcanzaste el límite de tasa: espera y reintenta.
`scan timed out`	Un manifiesto muy grande o con muchos avisos: divídelo en partes más pequeñas.

8 ¿Necesitas una clave o ayuda?

Solicita una clave, haz una pregunta o informa de un problema: estaremos encantados de ayudarte.

Contáctanos: cert-ix.com/contact · https://mcp.cert-ix.com/depcheck