

DepCheck MCP

User Guide

Everything you need to connect DepCheck to your AI coding agent and check dependencies for known vulnerabilities before they land in your code.

Free developer tool · Model Context Protocol

ENDPOINT:

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

Contents

- [1 Overview](#)
- [2 Connect your agent](#)
- [3 The five tools](#)
- [4 Reading a verdict](#)
- [5 How your data is handled](#)
- [6 Fair use & limits](#)
- [7 Troubleshooting](#)
- [8 Need a key or help?](#)

1 Overview

Everything you need to connect DepCheck to your AI coding agent and check dependencies for known vulnerabilities before they land in your code.

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

2 Connect your agent

First, request a free key at cert-ix.com/contact — we send you a key of the form `cixmcp_...` (no account needed). Then point your agent at the endpoint with that key.

Claude Code

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

Any MCP client (config file)

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

Works with Claude Code and any client that speaks MCP over HTTP. Once your key is active, your agent can call the tools immediately.

3 The five tools

check_package

Arguments: ecosystem name version

Check one package version for known vulnerabilities. Returns the advisories affecting exactly that version and the nearest safe version to upgrade to.

scan_dependencies

Arguments: manifest_content manifest_name

Scan a whole manifest at once — go.mod, package.json, package-lock.json, requirements.txt, pyproject.toml, Cargo.toml, Cargo.lock, pom.xml, composer.json. The hosted server takes the file body, never a path. Up to 2000 dependencies per scan.

suggest_safe_version

Arguments: ecosystem name

Get the newest version of a package that has zero known advisories.

get_advisory

Arguments: id

Pull the full detail of any advisory (GHSA-..., CVE-..., RUSTSEC-..., GO-...): description, CVSS, affected ranges and references.

get_cve_intel

Arguments: id

See exploitation intelligence for a CVE — CISA KEV status and EPSS score — to decide what to fix first. A KEV-listed or high-EPSS issue is being actively attacked and should jump the queue.

4 Reading a verdict

Field	Meaning
verdict	VULNERABLE or OK for the exact version checked.
advisories	Each with an id, severity and CVSS score.
exploitation	Flagged when the issue is on CISA KEV or has high EPSS — fix these first.
recommended_min_version	The nearest version above the current one that clears the advisories.

5 How your data is handled

- Nothing is stored. Your manifest is parsed in memory to extract package names and versions, then discarded — we keep neither your files nor your results.
- Only coordinates are checked — package name and version, never the contents of your files. Lookups are cached briefly in memory for speed.
- Sovereign mirror first. Checks run against our own advisory mirror hosted in EU infrastructure, so most lookups never leave Cert-IX.

Fallback egress: when the mirror can't answer a package with certainty, that package's name and version are looked up against the public OSV.dev API (operated by OpenSSF). So package coordinates — not file contents — may leave our infrastructure on that path. Keep this in mind if you check private or internal package names.

6 Fair use & limits

- Requests are rate-limited per key (roughly 20 per second). A full manifest scan is a single request.
- Keep your key private — one key per team or user. To rotate, request a new one and we retire the old.

7 Troubleshooting

Response	What it means
401 unauthorized	Missing or invalid key — check your Authorization: Bearer header.
429 too many requests	You hit the rate limit — back off and retry.
scan timed out	A very large or heavily-advised manifest — split it into smaller pieces.

8 Need a key or help?

Request a key, ask a question, or report an issue — we're happy to help.

Contact us: cert-ix.com/contact · <https://mcp.cert-ix.com/depcheck>

