Cert-IX

SERVER MCP · SICUREZZA DELLE DIPENDENZE

DepCheck MCP

Guida per l’utente

Tutto ciò che serve per collegare DepCheck al tuo agente di coding AI e controllare le dipendenze alla ricerca di vulnerabilità note prima che finiscano nel tuo codice.

Strumento gratuito per sviluppatori · Model Context Protocol

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

Indice

1 Panoramica

Tutto ciò che serve per collegare DepCheck al tuo agente di coding AI e controllare le dipendenze alla ricerca di vulnerabilità note prima che finiscano nel tuo codice.

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

2 Collega il tuo agente

Per prima cosa, richiedi una chiave gratuita su cert-ix.com/contact — ti inviamo una chiave nella forma cixmcp_… (nessun account necessario). Poi indirizza il tuo agente all'endpoint con quella chiave.

Claude Code

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

Qualsiasi client MCP (file di configurazione)

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

> Funziona con Claude Code e qualsiasi client che parla MCP su HTTP. Una volta attivata la chiave, il tuo agente può richiamare gli strumenti immediatamente.

3 I cinque strumenti

`check_package`

Argomenti: `ecosystem` `name` `version`

Controlla la versione di un pacchetto alla ricerca di vulnerabilità note. Restituisce le advisory che riguardano esattamente quella versione e la versione sicura più vicina a cui aggiornare.

`scan_dependencies`

Argomenti: `manifest_content` `manifest_name`

Analizza un intero manifest in una sola volta — go.mod, package.json, package-lock.json, requirements.txt, pyproject.toml, Cargo.toml, Cargo.lock, pom.xml, composer.json. Il server ospitato riceve il corpo del file, mai un percorso. Fino a 2000 dipendenze per scansione.

`suggest_safe_version`

Argomenti: `ecosystem` `name`

Ottieni la versione più recente di un pacchetto priva di advisory note.

`get_advisory`

Argomenti: `id`

Recupera tutti i dettagli di qualsiasi advisory (GHSA-…, CVE-…, RUSTSEC-…, GO-…): descrizione, CVSS, intervalli interessati e riferimenti.

`get_cve_intel`

Argomenti: `id`

Consulta l'intelligence sullo sfruttamento di un CVE — stato CISA KEV e punteggio EPSS — per decidere cosa correggere per primo. Un problema presente nella lista KEV o con EPSS elevato è attivamente sfruttato e dovrebbe passare in cima alla coda.

4 Lettura di un verdict

Campo	Significato
`verdict`	VULNERABLE o OK per la versione esatta controllata.
`advisories`	Ciascuna con un id, una gravità e un punteggio CVSS.
`exploitation`	Segnalato quando il problema è nella lista CISA KEV o ha un EPSS elevato — correggi questi per primi.
`recommended_min_version`	La versione più vicina superiore a quella attuale che elimina le advisory.

5 Come vengono gestiti i tuoi dati

- Non viene memorizzato nulla. Il tuo manifest viene analizzato in memoria per estrarre nomi e versioni dei pacchetti, poi scartato — non conserviamo né i tuoi file né i tuoi risultati.
- Vengono controllate solo le coordinate — nome e versione del pacchetto, mai il contenuto dei tuoi file. Le ricerche vengono memorizzate brevemente nella cache in memoria per velocità.
- Prima il mirror sovrano. I controlli vengono eseguiti sul nostro mirror di advisory ospitato in infrastruttura EU, così la maggior parte delle ricerche non lascia mai Cert-IX.

> Egress di fallback: quando il mirror non può rispondere con certezza su un pacchetto, il nome e la versione di quel pacchetto vengono cercati tramite l'API pubblica OSV.dev (gestita da OpenSSF). Quindi le coordinate del pacchetto — non il contenuto dei file — possono lasciare la nostra infrastruttura su quel percorso. Tienilo presente se controlli nomi di pacchetti privati o interni.

6 Uso corretto e limiti

- Le richieste sono soggette a limite di frequenza per chiave (circa 20 al secondo). Una scansione completa di un manifest è una singola richiesta.
- Mantieni privata la tua chiave — una chiave per team o utente. Per ruotarla, richiedine una nuova e noi ritiriamo quella vecchia.

7 Risoluzione dei problemi

Risposta	Cosa significa
`401 unauthorized`	Chiave mancante o non valida — controlla il tuo header Authorization: Bearer.
`429 too many requests`	Hai raggiunto il limite di frequenza — attendi e riprova.
`scan timed out`	Un manifest molto grande o con molte advisory — suddividilo in parti più piccole.

8 Ti serve una chiave o aiuto?

Richiedi una chiave, fai una domanda o segnala un problema — siamo felici di aiutarti.

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