BSIDESTLV 2026 · MAIN TRACK · 11 NOV

One Page to Rule Them All

Hijacking MCP Servers Using DNS Rebinding

Avishai Gonen · Yotam Perkal

one tab. no clicks.

WHO WE ARE

Two researchers, one browser tab

Avishai Gonen

- Bug bounty / vulnerability research - web, mobile, API
- [PLACEHOLDER - role, affiliation, one credibility line]

Yotam Perkal

- [PLACEHOLDER - role / team]
- [PLACEHOLDER - one credibility line]

ACT 1

The Building

The only genuinely new thing in this entire talk.

NEW

est. 2024

Powerful tools, sitting on localhost

- MCP exploded fast - servers everywhere, official and unofficial
- They expose real operational power: file systems, cloud APIs, CI runners
- Often **unauthenticated** - "it's local, so who cares"
- And now an **AI agent** is holding the trigger

100+

vulnerable MCP servers. One bug class.

Microsoft | CircleCI | JFrog | MongoDB | Elasticsearch | Grafana

“It’s on localhost, so only local apps can reach it.”

> This assumption was already false before MCP existed.
>
> **The promise of this talk: nothing that breaks it is new. Watch.**

ACT 2

The Door

DNS rebinding - the forgotten key that still fits the lock.

OLD

est. 2007 (Java-applet era)

DNS rebinding, refreshed

- Attacker controls the authoritative DNS for their own domain
- Short TTL - the name resolves to the attacker, then flips to **127.0.0.1**
- Same-origin policy keys on the **hostname**, not the underlying IP
- Result: attacker JS talks to your localhost service, same "origin"

ACT 2 · THE DOOR (OLD)

Why the browser may not save you

- Chrome's Private Network Access is meant to block exactly this
- But protection is **not consistent** across browsers
- Browser extensions with host permissions can change the picture

Short context for the demo - not a browser-internals deep dive.

ACT 2 · THE DOOR (OLD)

The fix is old too - and skipped anyway

Host allowlist

Validate the Host header. Reject anything unexpected.

Mandatory auth

Local is not a credential. Require one.

CORS ≠ fix

Why CORS does **not** solve this. [explain on deck]

Remember these - the case studies are servers that skipped them.

ACT 3

The Rooms

Decades-old bug classes - reached through the new door. Each room is bigger than the last.

OLD blast radius: reach › EXECUTE › IMPERSONATE › SCALE

From a webpage to remote code execution

- DNS rebinding opens the unauthenticated door – **GHSA-jwj7-74jh-p5c4**
- Unauth command injection (CWE-78) in **run_evaluation_tests** – GHSA-m9x7-h9px-p447, **CVSS 10.0**
- Payload lands in CircleCI’s own cloud runner → RCE
- The door is new; command injection is as old as it gets

LIVE DEMO 1

Rebind into CircleCI → command injection

One opened page. No extra interaction. A session the attacker now drives.

[PLACEHOLDER - demo steps, fallback recording, reset plan]

The server spends your credentials for you

- **docker/hub-mcp** holds your Personal Access Token server-side
- After rebind, the attacker page drives authenticated calls **as you**
- Enumerate private namespaces; **createRepository**, **updateRepositoryInfo**
- Token never appears in attacker JS – this is a **supply-chain** problem

LIVE DEMO 2

Rebind into Docker Hub → use the victim’s creds

Retrieve namespace and repo data with the server’s existing token.

[PLACEHOLDER - demo steps, fallback recording, reset plan]

Two servers down. How did we find 100+?

- [PLACEHOLDER - how you sourced / scanned the MCP ecosystem]
- [PLACEHOLDER - what signal flagged a server as vulnerable]
- [PLACEHOLDER - tooling / automation you built]

The pattern pointed to something upstream ...

One unsafe default, many victims

- **mark3labs/mcp-go** – 9,000+ GitHub stars
- Dispatches on HTTP method alone – no default Host / Origin allowlist
- Spoofed Host + Origin → establish a session, execute a tool, **no auth**
- Two downstream projects inherited it – incl. a **Microsoft-maintained** server
- Neither maintainer wrote the bug. The default spread it.

ACT 4

Nobody Checked the Foundation

The door is old. The rooms are old. Only the building is new.

door: 2007 | rooms: decades old | building: new

The classic bugs never left.

Command injection

SSRF

Path traversal

They just got a new door – and an AI agent to open it.

Take this home

- ✓ Require authentication - local is not a credential
- ✓ Validate Host **and** Origin headers
- ✓ Test browser-reachable transports
- ✓ Treat every local MCP server as external attack surface

2007 CALLED

The attack still works.

Because we keep rebuilding on foundations we never inspect.

Avishai Gonen · Yotam Perkal

[contact / handles / slides link]