مجلس الأمن السيبراني
CYBER SECURITY COUNCIL
United Arab Emirates

Critical RCE Vulnerability in MCP Inspector

Tracking #:432317435

Date:01-07-2025

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed the disclosure of a severe Remote Code Execution (RCE) flaw in the MCP Inspector, a core debugging tool within Anthropic's Model Context Protocol (MCP) framework.

TECHNICAL DETAILS:

A critical Remote Code Execution (RCE) **CVE-2025-49596** vulnerability was found in MCP Inspector, a debugging tool in Anthropic's Model Context Protocol (MCP) framework. This flaw allows malicious websites to execute commands on a developer's machine via a browser tab.

Vulnerability Details:

- **CVE:** CVE-2025-49596
- **Severity**: Critical (CVSS 9.4)
- **Affected Tool:** MCP Inspector (Anthropic)
- **Exploitation steps:**
  - Developer runs mcp dev command.
  - MCP Inspector listens on 0.0.0.0:6277.
  - Malicious site sends JavaScript payload to this port.
  - Payload executes arbitrary commands on the host machine.

Key Risks:

- **Unauthenticated access**: MCP Inspector runs without authentication or encryption by default.
- **CSRF via browser**: Exploits a long-standing browser flaw ("0.0.0.0-day") allowing websites to access localhost services.
- **Remote command execution**: Attackers can install malware, access files, or launch reverse shells.
- **Public exposure**: Some MCP Inspector instances are accessible online and vulnerable without browser interaction.

Fixed Versions:

- MCP Inspector v0.14.1+

RECOMMENDATIONS:

The UAE Cyber Security Council recommends applying the updates released by Anthropic.

Kindly circulate this information to your subsidiaries and partners as well as share with us any relevant information and findings.

The UAE Cyber Security Council extends its appreciation for the continued collaboration.

REFERENCES:

- https://nvd.nist.gov/vuln/detail/CVE-2025-49596