Arbitrary Android Intent Execution via mobile_open_url

High **gmegidish** published **GHSA-5qhv-x9j4-c3vm** 4 days ago

Package

@mobilenext/mobile-mcp (npm)

Affected versions

< 0.0.50

Patched versions

0.0.50

Description

Summary

The `mobile_open_url` tool in mobile-mcp passes user-supplied URLs directly to Android's intent system without any scheme validation, allowing execution of arbitrary Android intents, including USSD codes, phone calls, SMS messages, and content provider access.

Details

The vulnerable code passes URLs directly to `adb shell am start -a android.intent.action.VIEW -d <url>` without checking the URL scheme. This can enable malicious schemes such as `tel:`, `sms:`, `mailto:`, `content://`, and `market://` to be executed.

Since MCP servers are designed to be operated by AI agents, which are vulnerable to prompt injection attacks, a malicious document or website could inject instructions that cause the AI to execute dangerous intents on a connected mobile device.

Impact

An attacker via prompt injection can:

- Execute USSD codes (e.g., `tel:*#06#` to display IMEI - confirmed on Pixel 7a, behavior varies by device; or device-specific factory reset codes)
- Initiate phone calls to premium rate numbers
- Draft SMS messages with attacker-controlled content

- Access content providers (contacts, SMS, call logs)
- Open app installation prompts

Proof of Concept

```
{"jsonrpc":"2.0","id":1,"method":"tools/call","params":{"name":"mobile_open_url","
```

Result: IMEI displayed on device.

```
{"jsonrpc":"2.0","id":1,"method":"tools/call","params":{"name":"mobile_open_url","
```

Result: SMS app opens with a pre-filled message.

Remediation

Upgrade to version 0.0.50 or later, which restricts `mobile_open_url` to `http://` and `https://` schemes by default. Users who require other URL schemes can opt in by setting `MOBILEMCP_ALLOW_UNSAFE_URLS=1`.

References

- Fix: #299
- Release: https://github.com/mobile-next/mobile-mcp/releases/tag/0.0.50

Severity

High 8.3 / 10

CVSS v3 base metrics

Attack vector	Network
Attack complexity	Low
Privileges required	None
User interaction	Required
Scope	Unchanged
Confidentiality	Low
Integrity	High
Availability	High

Learn more about base metrics

CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:H/A:H

CVE ID

CVE-2026-35394

Weaknesses

▶ CWE-939

Credits

manthanghasadiya Reporter