Bug 2459131 (CVE-2026-6494) - CVE-2026-6494 aap-mcp-server: AAP MCP server: Log injection allows social engineering attacks via unsanitized input

Keywords: Security

Status: NEW

Alias: CVE-2026-6494

Product: Security Response

Component: vulnerability

Version: unspecified

Hardware: All

OS: Linux

Priority: medium

Severity: medium

Target Milestone: ---

Assignee: Product Security DevOps Team

QA Contact:

Docs Contact:

URL:

Whiteboard:

Depends On:

Blocks:

TreeView+ depends on / blocked

Reported: 2026-04-17 08:06 UTC by OSIDB Bzimport

Modified: 2026-04-17 08:09 UTC (History)

CC List: 11 users (show)

Fixed In Version:

Clone Of:

Environment:

Last Closed:

Embargoed:

Attachments (Terms of Use)

OSIDB Bzimport 2026-04-17 08:06:59 UTC Description

```
The AAP MCP server is vulnerable to multiple forms of log
injection because the :toolsetroute parameter is passed
directly to console.log()without prior sanitization,
validation, or neutralization of control characters. This
vulnerability exists across all six toolset-specific endpoints
(POST, GET, DELETE, and OPTIONS).  An unauthenticated remote
attacker can inject payloads containing newlines (%0A), tabs
(%09), and sophisticated ANSI escape sequences (e.g., \x1b[2J,
\x1b[31m). While the server's logging mechanism is append-
only, an attacker can use these characters to effectively hide
previous legitimate log entries from an operator's view and
replace them with fabricated, high-fidelity forged entries.

This capability facilitates advanced social engineering
```

attacks, where an operator might be tricked into executing dangerous commands or visiting malicious URLs in response to fabricated error messages.

Note

You need to log in before you can comment on or make changes to this bug.