

TACTICAL



AS105

UNEXPECTED CODE EXECUTION

A chatbot writes text for a human. An agent writes instructions for a machine.

CYBER SECURITY THAT STOPS HACKERS

// 01 // WHAT IT IS

OUTPUT REACHES SOMETHING THAT RUNS IT

A shell. An interpreter. A query engine. A build pipeline. The oldest rule in application security, arriving in a new place.

// WHERE IT LANDS

01

A SHELL

02

AN INTERPRETER

03

A QUERY ENGINE

04

A BUILD PIPELINE

// 02 // THE DOCUMENTED CASE

A DESIGN FLAW IN THE MODEL CONTEXT PROTOCOL

10 CVES

ISSUED AND COUNTING

15 APR 2026

PUBLISHED BY OX SECURITY

DESIGN LEVEL

UNSAFE TRANSPORT DEFAULTS

OX Security, published 15 April 2026. 10 CVEs issued and counting.

// 03 // THE SCALE

7,000+

PUBLICLY ACCESSIBLE SERVERS OBSERVED

Across implementations with more than 150 million downloads between them.

// WHAT WE DO NOT USE

A SEPARATE FIGURE OF 200,000 VULNERABLE INSTANCES IS THE RESEARCHERS' EXTRAPOLATION, NOT AN OBSERVATION. WE USE THE OBSERVED NUMBER.

// 04 // WHY SOUTH AFRICA

THE DEFAULTS ARE INHERITED

South African software houses build agent integrations for local banks, telecommunications operators and government. The protocol layer is shared. Nobody rewrites the transport configuration.

BANKS

TELECOMMUNICATIONS

GOVERNMENT

It was not one vendor's bug. It was a default that thousands of teams adopted at speed.

// 05 // THE POINT

NEVER TRUST OUTPUT AS INPUT

The rule has not changed. What changed is that the output is now fluent, confident, and arrives faster than a human can read it.

FLUENT

It reads as though a competent engineer wrote it.

CONFIDENT

Nothing in the output signals doubt, so nothing prompts review.

FASTER THAN REVIEW

It arrives faster than a human can read it.

// 06 // THREE QUESTIONS FOR MONDAY

THREE QUESTIONS FOR MONDAY

-
- 01** WHERE DOES AGENT OUTPUT REACH AN EXECUTION CONTEXT?
 - 02** WHO OWNS OUR MODEL CONTEXT PROTOCOL CONFIGURATION?
 - 03** WHEN DID ANYONE LAST LOOK AT ITS DEFAULTS?
-

THE FLAW WAS NOT IN THE CODE. IT WAS IN THE DEFAULT.

WE DO NOT RUN SCANS. WE DEPLOY OPERATORS.

// THE NEXT STEP

A THIRTY MINUTE DISCUSSION.

A no-obligation discussion to understand your requirement and to provide guidance on how NEWORDER can assist. No deployment, no commitment.

[BOOK DISCUSSION →](#)

EMAIL INFO@NEWORDERGROUP.NET · WEB WWW.NEWORDERGROUP.NET

NEXT: ASIO6 MEMORY AND CONTEXT POISONING