Horizon3.ai — LiteLLM chained with Starlette BadHost RCE

Contents

1 Horizon3.ai — LiteLLM chained with Starlette BadHost RCE

Field	Value
Reference key	`horizon3-chain`
Availability	AVAILABLE
Capture method	`primary`
Source type	remote_url
URL / path	https://horizon3.ai/attack-research/vulnerabilities/cve-2026-42271-chained-with-cve-2026-48710/
Captured (UTC)	2026-06-23T03:31:09Z
Content type	text/html; charset=UTF-8
HTTP status	200

1.1 Boardroom Citation Context

LiteLLM+Starlette chain; P7-05 tabletop.

1.2 Source Location

https://horizon3.ai/attack-research/vulnerabilities/cve-2026-42271-chained-with-cve-2026-48710/

1.3 Captured Content

```
CVE-2026-42271: LiteLLM Unauthenticated RCE | Horizon3.ai Skip to main content Skip to footer Ne
```

Archived reference article for AICSR-STUDY-2026-001 footnote corpus.