



Use Case Documentation

Uncoder AI

In production

Potential CVE-2024-35250 Exploitation Activity

```
1 title: Potential CVE-2024-35250 Exploitation Activity
2 id: 170e9373-2163-4a2c-90ba-f91e9ef7a8c1
3 status: experimental
4 description: 'Detects potentially suspicious loading of "ksproxy.ax", which may indicate
5 an attempt to exploit CVE-2024-35250.
6
7
8 references:
9 - https://thehackernews.com/2024/12/cisa-and-fbi-raise-aler
10 - https://github.com/varwara/CVE-2024-35250
11 - https://devco.re/blog/2024/08/23/streaming-vulnerabilitie
12 - https://www.cisa.gov/known-exploited-vulnerabilities-cata
13 author: '@eyezuhk Isaac Fernandes'
14 date: 2025-02-19
15 tags:
16 - attack.privilege-escalation
17 - attack.t1068
18 - cve.2024-35250
19 - detection.emerging-threats
20 logsource:
21 category: image_load
22 product: windows
23 detection:
24 selection:
25 ImageLoaded|endswith: \ksproxy.ax
26 filter_main_system_paths:
27 Image|startswith:
28 - C:\Program Files\
29 - C:\Program Files (x86)\
```

TIMELINE

AUDIT CONFIGURATION

Create Documentation

Choose a Confluence integration to create a page that documents the use case based on the intelligence and metadata of this rule.

Integration

Corp Confluence

Parent Page

Use Case Base

Cancel

Create Page

Use Case in your Confluence

+ Document

HotKeys

Automatically document use cases in your Confluence right from Uncoder AI.

- Set up integration once and use it on the fly
- All intelligence and metadata are saved together with code in a structured way
- Reduces time for use case management