**CVE-2022-0337 - Chromium System Environment Leakage**

**1. Một vài tìm hiểu ngắn gọn**

CVE-2022-0337 là một lỗ hổng bảo mật trong Chromium, trình duyệt mã nguồn mở được sử dụng làm nền tảng cho các trình duyệt phổ biến khác như Google Chrome, Microsoft Edge và Opera. Lỗ hổng này cho phép kẻ tấn công lấy được thông tin từ environment variables trên máy tính của người dùng thông qua việc người dùng thực hiện các hành động nhất định từ trang web độc hại do kẻ tấn công kiểm soát.

**Chi tiết kỹ thuật**:

* **Nguyên nhân**: Lỗ hổng này phát sinh do việc triển khai không đúng cách trong File System API của Google Chrome trên Windows, cụ thể là trong phương thức window.showSaveFilePicker().
* **Phương thức tấn công**: Kẻ tấn công tạo ra một trang HTML được thiết kế đặc biệt để khai thác lỗ hổng này. Khi người dùng truy cập trang web, mã JavaScript độc hại sẽ được thực thi, cho phép kẻ tấn công truy xuất các biến môi trường của hệ thống.
* **Phiên bản bị ảnh hưởng**: Tất cả các trình duyệt dựa trên nhân Chromium từ phiên bản 92 đến 96 đều bị ảnh hưởng, ngoại trừ Brave. Lỗ hổng đã được phát hiện trong phiên bản Chromium 92 và được vá trong phiên bản 97 (97.0.4692.71).

**2. Impact của CVE-2022-0337**

Lỗ hổng này dẫn đến rò rỉ thông tin hệ thống, cho phép kẻ tấn công truy xuất các biến môi trường của người dùng, chứa các thông tin nhạy cảm như thông tin cá nhân, cấu hình hệ thống, và các khóa API. Việc này có thể tạo điều kiện cho các cuộc tấn công tiếp theo, đặc biệt nếu các thông tin như API secret key bị lộ, có thể gây ra thiệt hại nghiêm trọng về bảo mật và tài chính cho người dùng.

**Hậu quả cụ thể**:

* **Rò rỉ thông tin cá nhân**: Các biến môi trường có thể chứa thông tin cá nhân và dữ liệu nhạy cảm.
* **Tấn công tiếp theo**: Thông tin bị rò rỉ có thể được sử dụng để thực hiện các cuộc tấn công khác như tấn công bằng API key, truy cập trái phép vào hệ thống hoặc dịch vụ.
* **Tổn thất tài chính**: Rò rỉ thông tin bảo mật như khóa API có thể dẫn đến việc mất mát tài chính hoặc thiệt hại danh tiếng cho người dùng hoặc tổ chức.

**3. Tái hiện CVE-2022-0337**

Nhóm em đã tái hiện thành công lỗ hổng này. Dưới đây là link video mô tả chi tiết quá trình tái hiện: [Link video tái hiện CVE-2022-0337](https://opswat2017-my.sharepoint.com/:v:/g/personal/trang_fellowship_opswat_com/EQbLwdkdSI1Kldj7YogSzOsBKIXLMyTrw47I3-tEVwhNIQ?nav=eyJyZWZlcnJhbEluZm8iOnsicmVmZXJyYWxBcHAiOiJPbmVEcml2ZUZvckJ1c2luZXNzIiwicmVmZXJyYWxBcHBQbGF0Zm9ybSI6IldlYiIsInJlZmVycmFsTW9kZSI6InZpZXciLCJyZWZlcnJhbFZpZXciOiJNeUZpbGVzTGlua0NvcHkifX0&e=GFxpQw)

Thông tin chi tiết về CVE-2022-0337 cũng được trình bày trong slide sau: [Link slide về CVE-2022-0337](https://opswat2017-my.sharepoint.com/:p:/g/personal/trang_fellowship_opswat_com/EeAQ1JXDyGFIqGqw8G5FwIUBl3MYrXiohG6PXZwMNaEtDA?e=beZ2nx)

**4. Khả năng phát hiện của OPSWAT Metadefender Endpoint**

OPSWAT Metadefender Endpoint có thể phát hiện CVE-2022-0337 và các lỗ hổng khác tồn tại trên các phiên bản Chrome từ 92 đến 97. Sản phẩm của OPSWAT cung cấp bản nâng cấp lên phiên bản Chrome mới nhất để khắc phục lỗ hổng này, đảm bảo an toàn cho người dùng.

**Cách thức hoạt động**:

* **Phát hiện**: Metadefender Endpoint liên tục quét các phiên bản trình duyệt để tìm kiếm các lỗ hổng đã biết, bao gồm CVE-2022-0337.
* **Cập nhật**: Khi phát hiện lỗ hổng, hệ thống sẽ thông báo và hướng dẫn người dùng nâng cấp trình duyệt lên phiên bản an toàn hơn.

**5. Khó khăn gặp phải**

Hiện tại, CVE-2022-0337 là một lỗ hổng đơn giản nên nhóm không gặp khó khăn gì trong quá trình nghiên cứu và tái hiện.