**Chuyên gia Việt phát hiện lỗ hổng nghiêm trọng của Windows**

Thứ sáu, 18/9/2020, 09:06 (GMT+7) <https://vnexpress.net/chuyen-gia-viet-phat-hien-lo-hong-nghiem-trong-cua-windows-4162224.html>

Chuyên gia Lê Hữu Quang Linh, 24 tuổi, ở Hà Nội, phát hiện ra lỗ hổng CVE-2020-1319 trên Windows và nhiều lần được Microsoft vinh danh.

Trên website của MSRC - Trung tâm phản hồi về bảo mật của Microsoft, Lê Hữu Quang Linh được nhắc đến là một trong những người phát hiện ra lỗ hổng CVE-2020-1319. Lỗ hổng này cho phép hacker chiếm quyền kiểm soát hệ thống từ xa, cài đặt chương trình, xem/thay đổi/xóa dữ liệu hoặc tạo tài khoản mới với đầy đủ quyền của người dùng.

Lỗ hổng xuất hiện trên 29 phiên bản Windows khác nhau, chủ yếu là Windows 10 và Windows Server, và đều được Microsoft đánh giá ở mức "Nguy cấp". Với việc phát hiện lỗi trên, Lê Hữu Quang Linh được hãng phần mềm Mỹ vinh danh thông qua chương trình Defense-in-depth đầu tháng 9.



Chuyên gia Lê Hữu Quang Linh được ghi nhận trên website của Microsoft.

Đây không phải lần đầu chuyên gia bảo mật sinh năm 1996 này phát hiện ra lỗ hổng của Microsoft. Hồi tháng 4 và tháng 6, Microsoft cũng vinh danh Linh nhờ việc phát hiện lỗ hổng có tên mã CVE-2020-0687 và CVE-2020-1299. Hai lỗ hổng này đều được đánh giá ở mức "Nguy cấp", cho phép kẻ tấn công tạo ra các tài khoản người dùng với đầy đủ quyền quản trị máy tính.

Nói về cách để tìm ra lỗi của hệ điều hành Windows, Linh cho biết anh thường xác định trước mục tiêu, sau đó nghiên cứu, theo đuổi mục tiêu đó một cách đủ lâu để có kết quả.

Hướng "tấn công" được Linh tìm ra từ việc theo dõi các nhà nghiên cứu đi trước, từ đó nắm bắt các lỗ hổng phổ biến của hệ điều hành Windows. Khi đã lựa chọn được mục tiêu, người thực hiện sẽ tìm "bề mặt" tấn công, sau đó ứng dụng kỹ thuật fuzzing để phát hiện lỗi. Fuzzing là kỹ thuật phát hiện lỗi tự động mà phần lớn các nhà nghiên cứu bảo mật hiện nay sử dụng. Tuy nhiên theo Linh, người nghiên cứu bảo mật cần hiểu rõ cách thức hoạt động của ứng dụng để tìm ra "bề mặt" tấn công chính xác.

Đánh giá về lỗi mới tìm ra, Quang Linh cho rằng lỗ hổng này tiềm ẩn nhiều nguy cơ, dù khả năng khai thác trong thực tế là chưa có. Tuy nhiên, "nếu thư viện xử lý media của Windows tồn tại nhiều lỗi tương tự, hacker có thể kết hợp các lỗi này để thực hiện một cuộc tấn công toàn diện, chiếm quyền điều khiển thiết bị", anh nói. Việc phát hiện ra lỗi này sẽ bảo vệ hàng triệu người dùng. Microsoft cho biết sẽ cập nhật bản vá để khắc phục lỗi trên bằng cách chỉnh sửa để Microsoft Windows Codecs Library xử lý các đối tượng trong bộ nhớ một cách chính xác.

Cách đây không lâu, Microsoft cũng đã vinh danh Lê Hữu Quang Linh trong top 100 nhà nghiên cứu bảo mật giá trị nhất của MSRC năm 2020. Anh đứng thứ 68, được ghi nhận là nhà nghiên cứu có sức ảnh hưởng lớn.

Ở tuổi 24, Quang Linh đã có nhiều năm kinh nghiệm nghiên cứu bảo mật. Anh từng có gần hai năm làm thực tập sinh tại Viettel; 1,5 năm làm việc tại VinCSS - đơn vị chuyên về bảo mật của VinGroup, và hiện giờ là nhà nghiên cứu bảo mật thuộc Trung tâm Giám sát an toàn không gian mạng quốc gia (NCSC), thuộc Cục An toàn thông tin, Bộ Thông tin và Truyền thông.



Lê Hữu Quang Linh đang làm việc tại Trung tâm Giám sát An toàn không gian mạng quốc gia. Ảnh: *NVCC.*

Ông Trần Quang Hưng, Giám đốc NCSC, đánh giá lĩnh vực an toàn, an ninh mạng tại Việt Nam vẫn còn non trẻ. "Nếu muốn Việt Nam trở thành cường quốc về an ninh mạng, con người là vấn đề tiên quyết", ông Hưng nói và kỳ vọng những nhân sự chất lượng cao như Lê Hữu Quang Linh sẽ góp phần hiện thực hóa mục tiêu này.

Trong 6 tháng qua, đội chuyên gia của NCSC cũng từng nhiều lần phát hiện ra các lỗ hổng bảo mật nghiêm trọng của các nền tảng lớn như Ủy ban châu Âu, thiết bị định tuyến D-link, công ty điện toán đám mây Rackspace, sàn TMĐT Alibaba.

**Lưu Quý**