BỘ THÔNG TIN VÀ TRUYỀN THÔNG
CỤC AN TOÀN THÔNG TIN

Số: 1038/CATTT-NCSC
V/v cảnh báo lỗ hổng trên trình duyệt Chrome

CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM
Độc lập - Tự do - Hạnh phúc

Hà Nội, ngày 04 tháng 11 năm 2019

Kính gửi:

- Đơn vị chuyên trách về CNTT các bộ, cơ quan ngang bộ, cơ quan thuộc Chính phủ;
- Sở Thông tin và Truyền thông các tỉnh, thành phố trực thuộc Trung ương;
- Các Tập đoàn, Tổng công ty nhà nước; Các tổ chức tài chính, ngân hàng;
- Người dùng không gian mạng Việt Nam.

Thực hiện chức năng, nhiệm vụ được giao, Cục An toàn thông tin thường xuyên thực hiện công tác theo dõi, giám sát trên Không gian mạng nhằm phát hiện và ngăn chặn sớm các nguy cơ gây mất ATTT.

Qua công tác theo dõi thông tin trên không gian mạng, và hoạt động hợp tác, chia sẻ thông tin với các tổ chức lớn về an toàn thông tin trong và ngoài nước, Cục An toàn thông tin ghi nhận xu hướng khai thác lỗ hổng (CVE-2019-13720) trong trình duyệt Google Chrome. Lỗ hổng này ảnh hưởng tới hầu hết các hệ điều hành (Microsoft Windows, Apple macOS và Linux) sử dụng trình duyệt Chrome trước phiên bản 78.0.3904.87.

Đây là lỗ hổng phép đối tượng tấn công chèn và thực thi mã lệnh từ xa một cách tự động. Do vậy tội phạm mạng có thể cài cắm mã khai thác vào các trang web người dùng hay truy cập hoặc lừa người dùng truy cập vào các trang này, người dùng truy cập các trang web này thì máy tính/thiết bị của người dùng sẽ bị tấn công, cài cắm mã độc. Lỗ hổng này đã được Google vá trong phiên bản Chrome 78.0.3904.87.

Nhằm bảo đảm an toàn thông tin và phòng tránh việc đối tượng tấn công lợi dụng điểm yếu an toàn thông tin để thực hiện những cuộc tấn công mạng nguy hiểm, Cục An toàn thông tin khuyến nghị các quản trị viên tại các cơ quan,

đơn vị thực hiện:

- Kiểm tra và cập nhật lên phiên bản Chrome mới nhất (78.0.3904.87) để vá lỗ hổng bảo mật và phòng tránh các nguy cơ bị tấn công thông qua việc khai thác lỗ hổng.

- Hạn chế truy cập các trang web, đường dẫn lạ đặc biệt là các trang web có trong phụ lục kèm theo đã bị cài cắm mã khai thác.

- Tại Việt Nam có 03 trình duyệt (Sfive, Chim Lạc và Cốc Cốc) phát triển trên mã nguồn Chromie cũng bị ảnh hưởng bởi lỗ hổng bảo mật này. Trong đó hai sản phẩm trình duyệt (Sfive, Chim Lạc) đã được đánh giá đáp ứng yêu cầu của TCVN 12637:2019 có khả năng cập nhật và cảnh báo khi người dùng truy cập các trang web độc hại (bao gồm cả những trang bị cài cắm mã khai thác trên) khi có cảnh báo Cục An toàn thông tin.

Trong trường hợp cần thiết có thể liên hệ đầu mối hỗ trợ của Cục An toàn thông tin: Trung tâm Giám sát an toàn không gian mạng quốc gia, điện thoại 02432091616, thư điện tử: ais@mic.gov.vn.

Trân trọng./.

Nơi nhận:
- Như trên;
- Bộ trưởng (để b/c);
- Thứ trưởng Nguyễn Thành Hưng (để b/c);
- Cục trưởng (để b/c);
- Lưu: VT, NCSC.

KT. CỤC TRƯỞNG
PHÓ CỤC TRƯỞNG

CỘNG HÒA X.H.C.N VIỆT NAM
CỤC AN TOÀN THÔNG TIN
BỘ THÔNG TIN VÀ TRUYỀN THÔNG

Nguyễn Khắc Lịch

Phụ lục
Một số hướng dẫn cập nhật bản vá

1. Danh sách trang web bị chèn mã khai thác

behindcorona.com

code.jquery.cdn.behindcorona.com

2. Hướng dẫn cập nhật bản vá

Mặc dù trình duyệt web Chrome tự động thông báo cho người dùng về phiên bản mới nhất có sẵn, người dùng được khuyến nghị kích hoạt thủ công quá trình cập nhật bằng cách :

Vào Menu/ Trợ giúp/ Giới thiệu về Google Chrome. Khi đó, trình duyệt sẽ tự động tải bản cập nhật và người dùng chỉ cần bấm "chạy lại"