SỞ THÔNG TIN VÀ TRUYỀN THÔNG CAO BẰNG
TRUNG TÂM CÔNG NGHỆ THÔNG TIN VÀ TRUYỀN THÔNG

Số: 100/TTCNTT&TT-KTCN
V/v cảnh báo lỗ hổng trên trình duyệt Chrome

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

Cao Bằng, ngày 18 tháng 11 năm 2019

Kính gửi:

- Văn phòng Tỉnh uỷ;
- Văn phòng HĐND tỉnh, Văn phòng UBND tỉnh;
- Các Sở, ban, ngành,UBND các huyện và thành phố.

Thực hiện công văn số 1038/CATTT-NCSC ngày 04 tháng 11 năm 2019 của Cục An toàn thông tin về việc cảnh báo lỗ hổng trên trình duyệt Chrome.

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 làm ảnh hưởng đến 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 cho 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 đến các trang web này thì máy tính/thiết bị của người dùng sẽ bị tấn công, cài cắm mã độc. Lỗ hổng này được Google vá trong phiên bản Chrome 78.0.3904.87.

Thực hiện chức năng, nhiệm vụ được giao, nhằm đảm bảo 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. Trung tâm Công nghệ thông tin và Truyền thông kính đề nghị các đơn vị chỉ đạo bộ phận chuyên môn khẩn cấp thực hiện:

1. 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 qua việc khai thác lỗ hổng.

2. 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.

3. Tại Việt Nam có 03 trình duyệt (Sfive, Chim lạc và Cốc Cốc) phát triển trên mã nguồn Chrome 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).

4. Nếu phát hiện mã độc tương tự cần nhanh chóng cô lập vùng/máy bị nhiễm và thông cáo về Trung tâm Công nghệ thông tin và Truyền thông Cao Bằng;

5. Khuyến cáo người sử dụng nâng cao cảnh giác, không mở và click vào các liên kết (link) cũng như các tập tin đính kèm trong email có chứa các tập tin dạng .doc, .pdf, .zip,… được gửi từ người lạ hoặc nếu email được gửi từ người quen nhưng cách đặt tiêu đề hoặc ngôn ngữ khác thường. Và cần thông báo cho bộ phận chuyên trách quản trị hệ thống hoặc đảm bảo an toàn thông tin khi nhận được email nghi ngờ.

Khi phát hiện sự cố hoặc cần giải đáp thông tin vui lòng thông báo về Trung tâm Công nghệ Thông tin và Truyền thông Cao Bằng, Sở Thông tin và Truyền thông Cao Bằng.

Địa chỉ: Số 009 Hoàng Văn Thụ, phường Hợp Giang, TP Cao Bằng;

Điện thoại: 0206 3 955 899;

Hòm thư điện tử tiếp nhận báo cáo sự cố: cbitc@caobang.gov.vn.

Rất mong nhận được sự quan tâm, phối hợp của quý cơ quan.

Trân trọng cảm ơn./.

Nơi nhận:
- Như trên;
- Phòng KTCGCN;
- Lưu VT.

GIÁM ĐỐC

Ký bởi: Trung tâm Công nghệ thông tin và truyền thông
Cơ quan: Tỉnh Cao Bằng
Thời gian ký: 18/11/2019 14:56:44

SỞ THÔNG TIN VÀ TRUYỀN THÔNG TỈNH CAO BẰNG
TRUNG TÂM CÔNG NGHỆ THÔNG TIN VÀ TRUYỀN THÔNG

Triệu Đình Thăng

PHỤ LỤC

MỘT SỐ HƯỚNG DẪN CẬP NHẬT BẢN VÁ

(Kèm theo công văn số /TTCNTT&TT-KTCN ngày 18 /11/2019 của Trung tâm Công nghệ thông tin và Truyền thông Cao Bằng)

1. **Danh sách các trang web bị hiễm 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".