BỘ KHOA HỌC VÀ CÔNG NGHỆ
TRUNG TÂM CÔNG NGHỆ THÔNG TIN

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

Số: 93 /TTCNTT-KTHT
V/v cảnh báo nguy cơ mất an toàn thông tin từ phần mềm họp trực tuyến Zoom

Hà Nội, ngày 17 tháng 04 năm 2020

Kính gửi: Các đơn vị trực thuộc Bộ

Nhằm tăng cường công tác bảo đảm an toàn, an ninh mạng và cảnh báo các nguy cơ mất an toàn thông tin cho các đơn vị trực thuộc Bộ, Trung tâm Công nghệ thông tin cảnh báo về các nguy cơ khi sử dụng phần mềm họp trực tuyến Zoom như sau:

Ngày 14/4/2020, Trung tâm ứng cứu khẩn cấp không gian mạng Việt Nam, Cục An toàn thông tin ghi nhận có hơn 500.000 tài khoản Zoom đã bị lộ lọt thông tin cá nhân của người sử dụng, trong đó bao gồm: email, mật khẩu, đường dẫn URL các cuộc họp và mật khẩu kèm theo.

Hiện nay, Zoom đang là phần mềm phổ biến cho học trực tuyến, tổ chức hội họp và làm việc từ xa. Tuy nhiên, phần mềm này tồn tại một số lỗ hổng bảo mật nghiêm trọng như: mã hóa dữ liệu đầu cuối kém, dễ dàng bị dò quét ID cuộc họp, lỗ hổng liên quan đến đường dẫn UNC (Universal Naming Convention).

Từ đầu năm 2020, nhiều lỗ hổng bảo mật của Zoom đã được công bố mã lỗ hổng (trong đó có lỗ hổng chưa được nhà cung cấp xử lý triệt để) như: CVE-2020-11500, CVE-2020-11469, CVE-2020-11470, ... với nhiều mức độ nguy hiểm khác nhau *(chi tiết tại phụ lục kèm theo)*.

Thông qua những lỗ hổng trên, tin tặc có thể truy cập bất hợp pháp vào các phòng họp, theo dõi, truyền bá các thông tin xấu độc hại, đánh cắp thông tin hoặc cài đặt mã độc trực tiếp trên máy tính người dùng.

Để tăng cường công tác bảo đảm an toàn, an ninh mạng, đặc biệt là bảo vệ thông tin cá nhân, bảo vệ quyền và lợi ích hợp pháp của các đơn vị trực thuộc Bộ và người sử dụng, Trung tâm Công nghệ thông tin khuyến cáo:

1. Các đơn vị trực thuộc Bộ không nên sử dụng phần mềm Zoom để phục vụ các buổi họp trực tuyến tại đơn vị mình.

2. Ưu tiên lựa chọn các sản phẩm phần mềm họp trực tuyến và làm việc từ xa do Trung tâm Công nghệ thông tin cung cấp hoặc các doanh nghiệp uy tín sản xuất.

3. Đối với người sử dụng các phần mềm học trực tuyến, tổ chức hội họp và làm việc từ xa:

- Chú ý tải phần mềm từ các nguồn chính thống, thường xuyên cập nhật phiên bản mới nhất của phần mềm.

- Không chia sẻ thông tin về phòng họp (ID, mật khẩu) để tránh các trường hợp bị kẻ xấu theo dõi, phá hoại.

- Thiết lập các cấu hình bảo mật cao trên các phần mềm họp trực tuyến. Cụ thể: đặt mật khẩu phức tạp cho các buổi họp; kích hoạt chế độ xét duyệt người tham gia trước khi vào phòng họp; thiết lập các tính năng quản lý việc chia sẻ màn hình trong buổi họp; hạn chế việc lưu lại nội dung buổi họp trong trường hợp không cần thiết.

- Đối với người dùng đã sử dụng phần mềm Zoom, thực hiện ngay việc đổi mật khẩu phức tạp, tránh sử dụng chung mật khẩu với các tài khoản khác.

- Khi phát hiện nguy cơ, dấu hiệu lộ, lọt thông tin cá nhân của người sử dụng, cần nhanh chóng khắc phục và kịp thời thông báo cho Trung tâm Công nghệ thông tin và các cơ quan chức năng có thẩm quyền liên quan để phối hợp xử lý kịp thời các vấn đề phát sinh.

Đầu mối liên hệ: Phòng Kỹ thuật hạ tầng, Trung tâm Công nghệ thông tin, điện thoại 02439439060, email: phongktht@most.gov.vn.

Trân trọng./.

Nơi nhận:
- Như trên;
- Thứ trưởng Bùi Thế Duy (để b/c);
- Lưu: VP, KTHT.

GIÁM ĐỐC

BỘ KHOA HỌC VÀ CÔNG NGHỆ
TRUNG TÂM CÔNG NGHỆ THÔNG TIN

Ký bởi: Trung tâm Công nghệ thông tin
Cơ quan: Bộ Khoa học và Công nghệ
Ngày ký: 18.04.2020 10:50:55 +07:00

Hà Quốc Trung

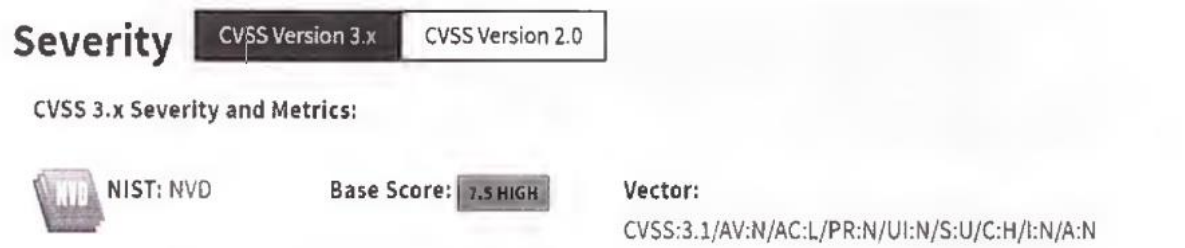
PHỤ LỤC

Các mã lỗi quốc tế đã được công bố đối với phần mềm Zoom

(Kèm theo Công văn số /TTCNTT-KTHT ngày /4/2020)

1. Mã lỗi: CVE-2020-11500 (Chưa có bản vá)

Mức độ lỗi: Mức cao

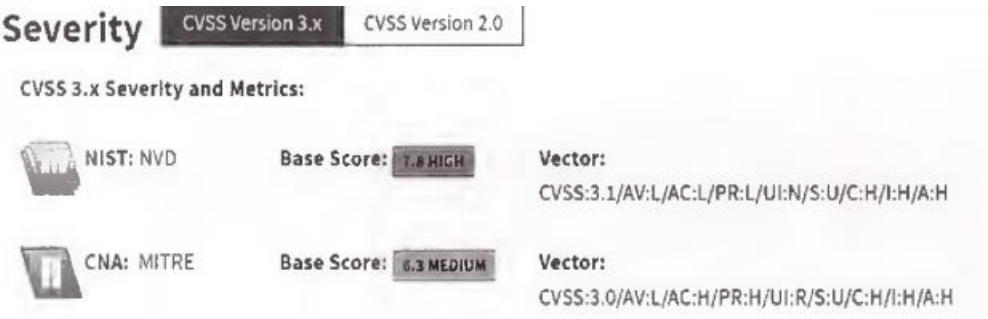


Mô tả lỗi:

Cho đến phiên bản 4.6.9 của Zoom Client có sử dụng chế độ ECB của thuật toán mã hóa AES với khóa 128 bít để mã hóa video và âm thanh khi truyền đi. Chế độ ECB được đánh giá là chế độ mã hóa yếu nhất trong các chế độ có sẵn của AES, có thể cho phép tin tặc có thể xem được hình ảnh trong cuộc họp.

2. Mã lỗi: CVE-2020-11469

Mức độ lỗi: Mức cao



Mô tả lỗi:

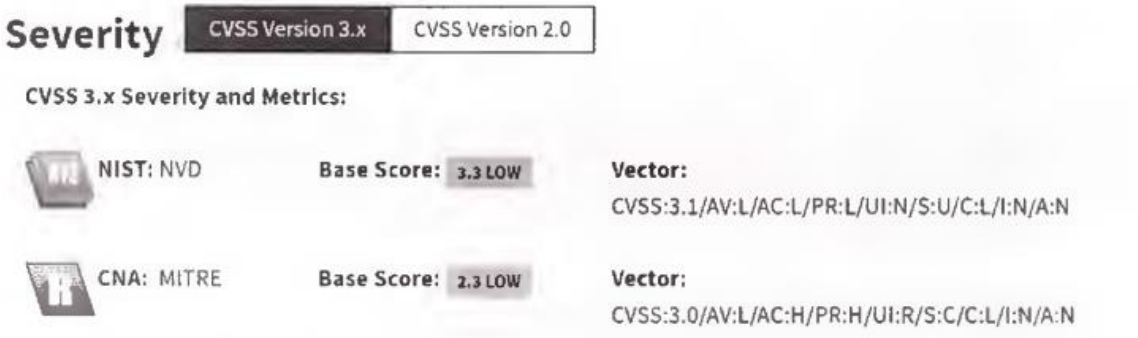
Phiên bản 4.6.8 trở về trước của Zoom Client được phát hiện có lỗ hổng trên hệ điều hành macOS và được phân loại là nghiêm trọng. Lỗ hổng này cho phép kẻ tấn công sao chép tập tin runwithroot vào thư mục tạm thời của người dùng trong khi cài đặt, cho phép tin tặc được quyền truy cập root bằng cách thay thế runwithroot. Tin tặc sau đó chiếm được quyền quản trị cao nhất trong máy bị tấn công.

Khuyến nghị:

Cập nhật phiên bản 4.6.9 trở lên.

3. Mã Lỗi: CVE-2020-11470

Mức độ lỗi: Mức thấp



Mô tả lỗi:

Phiên bán 4.6.8 trở về trước của Zoom Client được phát hiện có lỗ hổng trên hệ điều hành macOS cho phép vô hiệu hóa thư viện xác thực. Từ đó cho phép quyền truy cập camera và micro của nạn nhân trái phép.

Khuyến nghị:

Cập nhật phiên bản 4.6.9 trở lên.