UBND TỈNH QUẢNG TRỊ
SỞ THÔNG TIN VÀ TRUYỀN THÔNG

Số:279/STTTT-CNTT

V/v cảnh báo nguy cơ mất an toàn thông tin từ phần mềm họp trực tuyến Zoom

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

Quảng Trị, ngày 17 tháng 4 năm 2020

Kính gửi:

- Văn phòng UBND tỉnh;
- Các Sở, ban, ngành cấp tỉnh;
- UBND các huyện, thị xã, thành phố.

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 việc triển khai 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 nhằm theo dõi, truyền bá các thông tin xấu độc, đánh cắp thông tin hoặc cài đặt mã độc trực tiếp trên máy tính người dùng.

Thực hiện Chỉ thị số 14/CT-TTg ngày 25/5/2018 của Thủ tướng Chính phủ về Nâng cao năng lực phòng, chống phần mềm độc hại; Chỉ thị số 14/CT-TTg ngày 07/6/2019 của Thủ tướng Chính phủ về việc tăng cường bảo đảm an toàn, an ninh mạng nhằm cải thiện chỉ số xếp hạng của Việt Nam; Quyết định số 05/2017/QĐ-TTg ngày 16/03/2017 của Thủ tướng Chính phủ về việc ban hành quy định về hệ thống phương án ứng cứu khẩn cấp bảo đảm an toàn thông tin mạng quốc gia; Thông tư số 20/2017/TT-BTTTT ngày 12/9/2017 của Bộ Thông tin và Truyền thông quy định về điều phối, ứng cứu sự cố an toàn thông tin mạng toàn quốc và Chương trình hành động số 161-CTHĐ/TU ngày 19/8/2019 của Ban Thường vụ Tỉnh ủy về việc thực hiện Nghị quyết số 30-NQ/TW ngày 25/7/2018 của Bộ Chính trị về Chiến lược An ninh mạng quốc gia; nhằm 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 cơ quan, tô chức và người sử dụng, Sở Thông tin và Truyền thông khuyến cáo:

1. Các cơ quan, tổ chức hành chính nhà nước không nên sử dụng phần mềm Zoom để phục vụ các buổi họp trực tuyến tại đơn vị mình. Đối với các tổ chức, cá nhân khác cần cân nhắc cẩn thận khi sử dụng phần mềm họp trực tuyến Zoom cho các hoạt động học trực tuyến, trao đổi trực tuyến hoặc các tổ chức hội họp khác..

2. Ưu tiên lựa chọn các sản phẩm phần mềm học trực tuyến, tổ chức hội họp và làm việc từ xa do doanh nghiệp uy tín sản xuất, đặc biệt là các sản phẩm do doanh nghiệp uy tín trong nước cung cấp như: Viettel, VNPT, Mobifone, FPT,VNG, CMC, Nhân Hòa,...

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.

Mọi vướng mắc vui lòng liên hệ: Sở Thông tin và Truyền thông - Thành viên mạng lưới Ứng cứu sự cố mạng Internet Việt Nam do Bộ Thông tin và Truyền thông thành lập. Đơn vị thường trực kỹ thuật: Trung tâm Công nghệ thông tin và Truyền thông, điện thoại 0233. 3504909./.

Nơi nhận:
- Như trên;
- UBND tỉnh (báo cáo);
- Phòng PA03 - Công an tỉnh (PH);
- Trung tâm CNTT-TT (phối hợp thực hiện);
- Lưu: VT, CNTT.

KT. GIÁM ĐỐC
PHÓ GIÁM ĐỐC

CỘNG HÒA X.H.C.N VIỆT NAM
SỞ THÔNG TIN VÀ TRUYỀN THÔNG
TỈNH QUẢNG TRỊ

Người ký: Nguyễn Thị Huyền
Email: nguyenthihuyenqt@quangtri.gov.vn
Cơ quan: Sở Thông tin và Truyền thông, Tỉnh Quảng Trị
Chức vụ: Phó Giám đốc
Thời gian ký: 17.04.2020 07:27:09 +07:00

Nguyễn Thị Huyền

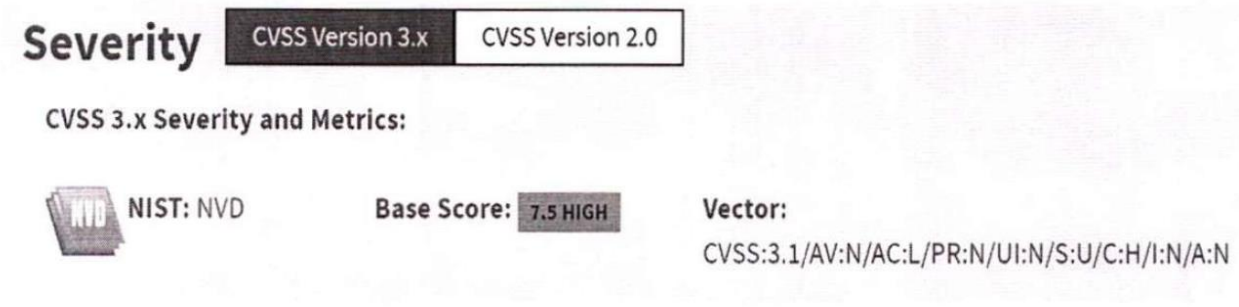
PHỤ LỤC

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

(Kèm theo công văn số 279/STTTT- CNTT ngày 17/4/2020 của Sở Thông tin và Truyền thông)

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

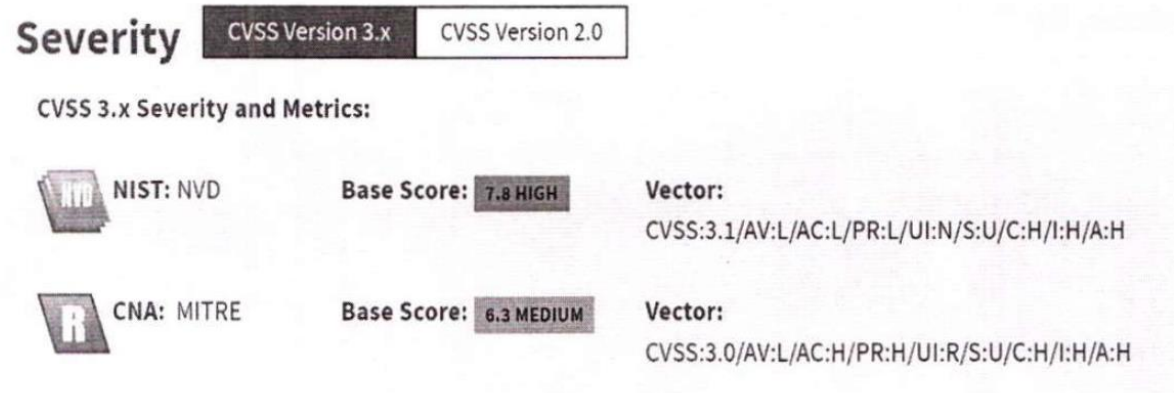
Mức độ lỗi: Mức Cao



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



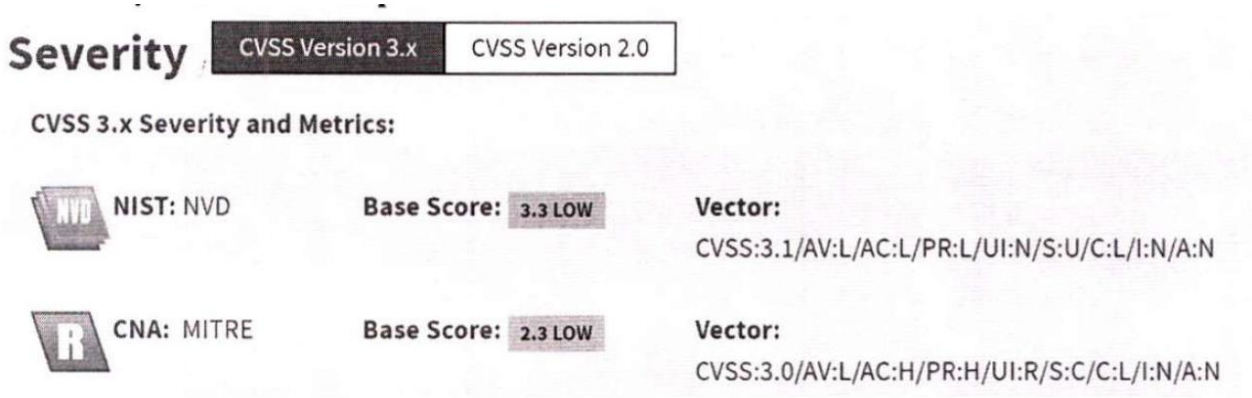
Mô tả lỗi: Phiên bản 4.6.8 trở về trước của Zoom Client được phát hiện có lỗ hổng trên hệ điều hành macOS và được phân loại là nghiêm trọng. Lỗ hổng này cho phép kẻ tấn công sao chép tập tin runwithroot vào thư mục tạm thời của người dùng trong khi cài đặt, cho phép tin tặc được quyền truy cập root bằng 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 bản 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.