

Số: 250/CATTT-VNCERT/CC

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

Hà Nội, ngày 14 tháng 4 năm 2020

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 Ngân hàng TMCP; Các tổ chức tài chính;
- Hệ thống các đơn vị chuyên trách về an toàn thông tin;
- Các doanh nghiệp, tổ chức, cá nhân khác.

Nhằm tăng cường công tác bảo đảm an toàn, an ninh mạng cho các hệ thống thông tin trong cơ quan hành chính Nhà nước và cảnh báo các nguy cơ mất an toàn thông tin cho các Bộ, ngành, địa phương, các tổ chức và cá nhân, Cục An toàn 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, 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 cơ quan, tổ chức, doanh nghiệp và người sử dụng, Cục An toàn thông tin 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 doanh nghiệp, tổ chức, cá nhân khác cần nhắc nhở 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 các doanh nghiệp cung cấp phần mềm học trực tuyến, tổ chức hội họp và làm việc từ xa: phải trang bị đầy đủ các tính năng bảo mật cho phần mềm, bảo đảm an toàn thông tin cho người sử dụng, có đội ngũ kỹ thuật để hỗ trợ kịp thời cho khách hàng.

4. 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 Cục ATTT 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: Trung tâm Ứng cứu khẩn cấp không gian mạng Việt Nam, Cục An toàn thông tin, điện thoại: 086 9100320, email: office@vncert.vn./.

Nơi nhận:

- Như trên;
- Bộ trưởng (để b/c);
- Thứ trưởng Nguyễn Thành Hưng (để b/c);
- Cục trưởng (để b/c);
- Trung tâm NCSC;
- Lưu: VT, VNCERT/CC.

**KT. CỤC TRƯỞNG
PHÓ CỤC TRƯỞNG**



Nguyễn Khắc Lịch

PHỤ LỤC


Các mã lỗi quốc tế đã được công bố đối với phần mềm Zoom
(Kèm theo công văn số 250 /CATT-VNCERT/CC ngày 14/4/2020)

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

Mức độ lỗi: Mức Cao

Severity CVSS Version 3.x CVSS Version 2.0

CVSS 3.x Severity and Metrics:

 NIST: NVD Base Score: 7.5 HIGH Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N

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 bit 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

Severity CVSS Version 3.x CVSS Version 2.0

CVSS 3.x Severity and Metrics:

 NIST: NVD Base Score: 7.8 HIGH Vector: CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H

 CNA: MITRE Base Score: 6.3 MEDIUM Vector: CVSS:3.0/AV:L/AC:H/PR:H/UI:R/S:U/C:H/I:H/A:H

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

Severity CVSS Version 3.x CVSS Version 2.0

CVSS 3.x Severity and Metrics:



NIST: NVD

Base Score: 3.3 LOW

Vector:

CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:L/I:N/A:N



CNA: MITRE

Base Score: 2.3 LOW

Vector:

CVSS:3.0/AV:L/AC:H/PR:H/UI:R/S:C/C:L/I:N/A:N

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.