

Số: /VP

Đông Đa, ngày tháng năm 2024

V/v cảnh báo lỗ hổng CVE-2024-0819  
trong phần mềm Team Viewer.

Kính gửi :

- Các phòng, ban, đơn vị thuộc quận;
- UBND 21 phường.

Thực hiện Công văn số 740/STTTT-ATTT&GDĐT ngày 27/03/2024 của Sở Thông tin và Truyền thông v/v cảnh báo lỗ hổng CVE-2024-0819 trong phần mềm Team Viewer; nhằm bảo đảm an toàn thông tin, an ninh mạng cho các hệ thống, Văn phòng HĐND&UBND quận đề nghị các phòng, ban, đơn vị, UBND 21 phường một số nội dung sau:

1. Kiểm tra, rà soát, xác định máy tính sử dụng phần mềm Team Viewer có khả năng bị ảnh hưởng bởi các lỗ hổng bảo mật .

**Hướng dẫn khắc phục** : nâng cấp phần mềm Team Viewer lên **trên** phiên bản 15.51.5 (Tham khảo tham khảo phụ lục Công văn số 2257/CAHN-PA05 của Công an Thành phố Hà Nội gửi kèm theo) và áp dụng một số biện pháp bảo mật bổ sung sau :

- Đặt mật khẩu tùy chọn (Options) mạnh (Mật khẩu có độ dài ít nhất 12 ký tự, trong đó có ít nhất 1 chữ viết hoa, một chữ số và một ký tự đặc biệt) cho tài khoản Team Viewer.

- Trong Team Viewer, bật "Changes require administrative rights on this computer" (các thay đổi yêu cầu quyền quản trị trên máy tính) giúp kiểm soát chặt chẽ hơn đối với các cài đặt nhạy cảm.

- Sử dụng xác thực 2 bước và áp dụng danh sách Block&Allow để giới hạn quyền truy cập.

2. Chủ động, tăng cường giám sát các hệ thống thông tin của cơ quan, sẵn sàng phương án xử lý khi phát hiện có dấu hiệu khai thác, tấn công mạng; đồng thời thường xuyên theo dõi kênh cảnh báo của các cơ quan chức năng, các tổ chức lớn về an toàn thông tin để phát hiện kịp thời nguy cơ tấn công mạng và các lỗ hổng bảo mật.

Kết quả kiểm tra, rà soát, khắc phục gửi về Văn phòng HĐND& UBND quận Đống Đa *trước ngày 09/4/2024* (Đ/c Đỗ Thùy Linh , số điện thoại 0983.529.978, email: dothuylinh\_dongda@hanoi.gov.vn).

*Nơi nhận:*

- Như trên;

- Lưu: VP.

**CHÁNH VĂN PHÒNG**

**Nguyễn Trọng Hải**