UBND TỈNH LÀO CAI
SỞ THÔNG TIN VÀ TRUYỀN THÔNG

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

Số: 852 /STTTT-BCVTCNTT
V/v cảnh báo lỗ hổng nguy hiểm trên máy chủ Domain Controller.

Lào Cai, ngày 17 tháng 9 năm 2020

Kính gửi:
- Văn phòng: Tỉnh ủy, HĐND tỉnh, UBND tỉnh;
- Các Sở, ban, ngành;
- UBND các huyện, thị xã, thành phố;
- Viettel Lào Cai, VNPT Lào Cai.

Thực hiện Chỉ thị số 12/CT-UBND ngày 09/9/2020 của UBND tỉnh về việc tăng cường đảm bảo an toàn, an ninh thông tin mạng trong các cơ quan nhà nước trên địa bàn tỉnh Lào Cai. Ngày 11/8/2020, hãng Microsoft đã công bố lỗ hổng CVE-2020-1472 (còn được gọi là Zerologon) trên các máy chủ Domain Controller, qua công tác theo dõi, giám sát an toàn thông tin và trên cơ sở khuyến nghị của các đơn vị chuyên trách về An toàn thông tin mạng đã phát hiện một số mã khai thác lỗ hổng được công khai trên mạng Internet và một số nhóm APT có dấu hiệu tận dụng lỗ hổng này để tấn công sâu vào hệ thống thông tin của các cơ quan tổ chức.

Theo đánh giá sơ bộ, lỗ hổng này có thể ảnh hưởng đến nhiều cơ quan, tổ chức ở Việt Nam, đặc biệt là cơ quan chính phủ, ngân hàng, tổ chức tài chính, tập đoàn, doanh nghiệp và các công ty lớn triển khai mô hình mạng có sử dụng máy chủ Domain Controller. Sở Thông tin và Truyền thông đề nghị các cơ quan, đơn vị, địa phương có triển khai mô hình mạng có sử dụng máy chủ Domain Controller thực hiện một số khuyến nghị như sau:

1. Thực hiện kiểm tra, rà soát và có giải pháp, phương án ngăn chặn các nhóm đối tượng tấn công lợi dụng lỗ hổng (CVE-2020-1472) để thực hiện tấn công APT nguy hiểm.

2. Tăng cường giám sát và sẵn sàng phương án xử lý khi có dấu hiệu bị khai thác, tấn công mạng. Các cơ quan, đơn vị có nhân sự kỹ thuật tốt có thể thử nghiệm tấn công xâm nhập vào hệ thống qua lỗ hổng này để có các biện pháp phòng chống tấn công mạng hiệu quả.

3. Giao Trung tâm CNTT và Truyền thông thực hiện rà soát các hệ thống thông tin tại Trung tâm mạng thông tin của tỉnh; Đề nghị VNPT Lào Cai, Viettel Lào Cai chủ động thực hiện rà soát các dịch vụ CNTT do đơn vị đang cung cấp trên địa bàn tỉnh.

Trong trường hợp cần thiết có thể liên hệ đầu mối hỗ trợ của Sở Thông tin và Truyền thông, Tổ ứng cứu sự cố máy tính của tỉnh: điện thoại 02143.828.669/02143.841.288, thư điện tử: cert@laocai.gov.vn.

Trên đây là Cảnh báo lỗ hổng nguy hiểm trên máy chủ Domain Controller, Sở Thông tin và Truyền thông khuyến nghị các cơ quan, đơn vị, địa phương và doanh nghiệp quan tâm, phối hợp thực hiện./.

Nơi nhận:
- UBND tỉnh (b/c);
- Như trên;
- Lãnh đạo sở;
- TT.CNTT&TT (rà soát, thực hiện);
- Lưu: VT, BCVTCNTT.

KT. GIÁM ĐỐC
PHÓ GIÁM ĐỐC

CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM
SỞ THÔNG TIN VÀ TRUYỀN THÔNG
TỈNH LÀO CAI

Sở Thông tin và Truyền thông
17-09-2020 10:29:07 +07:00

Tăng Văn Hạnh