UBND TỈNH BÌNH THUẬN
SỞ Y TẾ

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

Số: 4068 /SYT-VP

Bình Thuận, ngày 01 tháng 12 năm 2020

V/v cảnh báo nguy cơ tấn công mạng, khai thác lỗ hổng bảo mật trên thiết bị DrayTek

Kính gửi: Các cơ quan, đơn vị trực thuộc

Thực hiện Công văn số 823/CNTT-YTDT ngày 30/11/2020 của Cục công nghệ thông tin - Bộ Y tế về việc cảnh báo nguy cơ tấn công mạng, khai thác lỗ hổng bảo mật trên thiết bị DrayTek;

Theo đó, ngày 03/11/2020, Bộ Công an có ban hành Công văn số 47/TB-BCA-A05 về việc cảnh báo nguy cơ tấn công có chủ đích (APT) thông qua khai thác lỗ hổng bảo mật trên một số dòng thiết bị DrayTek, cụ thể như sau:

- Theo công bố từ tháng 2/2020 của các hãng bảo mật trên thế giới và của Draytek, một số thiết bị định tuyến và chuyển mạch của hãng này có lỗ hổng bảo mật nghiêm trọng (mã lỗi CVE-2020-8515). Tin tặc khai thác thành công lỗ hổng bảo mật này có thể đạt quyền truy cập cao nhất (quyền root) vào thiết bị. Đặc biệt nguy hiểm với các thiết bị định tuyến, thường được sử dụng là điểm kết nối giữa mạng Internet với hệ thống mạng cục bộ (LAN) bên trong. Bên cạnh các thiết bị định tuyến, một số thiết bị chuyển mạch của hãng này có lỗ hổng cũng kéo theo nguy cơ bị tin tặc tấn công, thay đổi cấu hình VLAN, cho phép tin tặc truy cập các phân vùng mạng được bảo vệ trong hệ thống mạng cục bộ.

- Danh sách các thiết bị DrayTek tồn tại lỗ hổng bảo mật CVE-2020-8515:

STT	Tên thiết bị	Phiên bản Firmware
1	DrayTek Vigor2960	< 1.5.1
2	DrayTek Vigor300B	< 1.5.1
3	DrayTek Vigor3900	< 1.5.1
4	DrayTek VigorSwitch20P2121	< 2.3.2
5	DrayTek VigorSwitch20G1280	< 2.3.2
6	DrayTek VigorSwitch20P1280	< 2.3.2
7	DrayTek VigorSwitch20G2280	< 2.3.2
8	DrayTek VigorSwitch20P2280	< 2.3.2

Nhằm đảm bảo an toàn thông tin cho các hệ thống thông tin ngành y tế, Sở Y tế đề nghị các cơ quan, đơn vị trực thuộc thực hiện một số nội dung, cụ thể như sau:

- Tổ chức kiểm tra, rà soát các thiết bị DrayTek (nếu có) được sử dụng trong hệ thống mạng, kiểm tra cấu hình, cập nhật phiên bản Firmware mới nhất, xóa bỏ các tài khoản lạ, tắt tính năng quản trị từ xa qua mạng Internet (nếu không cần thiết). Thống kê số lượng, danh sách các thiết bị DrayTek đang sử dụng tại cơ quan, đơn vị.

- Tăng cường giám sát an ninh mạng, kịp thời phát hiện tấn công mạng, phối hợp với các cơ quan chức năng trong việc xác minh, xử lý đối tượng thực hiện tấn công mạng.

- Kết quả kiểm tra, rà soát gửi về Sở Y tế trước ngày **04/12/2020** để Sở tổng hợp, báo cáo Cục Công nghệ thông tin- Bộ Y tế; các cơ quan, đơn vị không sử dụng các thiết bị DrayTek cũng báo cáo bằng văn bản là tại cơ quan, đơn vị không sử dụng các thiết bị DrayTek. Báo cáo gửi trước về địa chỉ mail công vụ: *thanhtt@syt.binhthhuan.gov.vn*.

Đề nghị các cơ quan, đơn vị trực thuộc khẩn trương triển khai thực hiện các nội dung trên./.

Nơi nhận:
- Như trên;;
- Lưu: VT, VP.

GIÁM ĐỐC

Người ký: Sở Y tế tỉnh Bình Thuận
Thời gian ký: 01.12.2020 15:06:51 +07:00

Nguyễn Quốc Việt