BỘ KHOA HỌC VÀ CÔNG NGHỆ
TRUNG TÂM CÔNG NGHỆ THÔNG TIN

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

Số: 336 /TTCNTT-KTHT
V/v hoạt động tấn công mạng, khai thác lỗ hổng

Hà Nội, ngày 10 tháng 11 năm 2020

Kính gửi: Các đơn vị trực thuộc Bộ

Hiện tại Bộ Công an phát hiện nhiều nhóm tội phạm mạng gia tăng hoạt động tấn công có chủ đích (APT) thông qua khai thác lỗ hổng bảo mật trên một số dòng thiết bị DrayTek, ảnh hưởng trực tiếp đến an ninh mạng, an toàn thông tin của các cơ quan, tổ chức, bộ, ban, ngành, nội dung cụ thể như sau:

1. 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 danh sách kèm theo)* 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. Sau khi kiểm soát thiết bị này, tin tặc có thể rà quét, thu thập thông tin hệ thống mạng; nghe trộm dữ liệu trên đường truyền để thu thập thông tin tài khoản đăng nhập với các giao thức không mã hóa; chỉnh sửa cấu hình, chuyển hướng truy cập mạng nhằm cài cắm mã độc vào các máy chủ, máy trạm bên trong; tiếp tục mở rộng tấn công, kiểm soát hệ thống mạng; thu thập tài liệu nội bộ, bí mật nhà nước hoặc xóa, mã hóa dữ liệu đòi tiền chuộc gây thiệt hại lớn cho các cơ quan, tổ chức. 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.

Qua điều tra hoạt động tấn công mạng, Bộ Công an nhận thấy thời gian qua đã có nhiều cơ quan, doanh nghiệp bị tấn công mạng thông qua lỗ hổng bảo mật trên thiết bị mạng DrayTek. Mặc dù hãng DrayTek đã phát hành bản cập nhật phần sụn (Firmware) cho các sản phẩm có lỗ hổng bảo mật, tuy nhiên, đến nay vẫn có khoảng **2453** thiết bị định tuyến DrayTek Vigor kết nối Internet ở Việt Nam có thể tồn tại lỗ hổng bảo mật, chưa được cập nhật bản vá. Nếu không xử lý, khắc phục kịp thời có thể là mục tiêu tấn công của các nhóm tội phạm mạng.

2. Từ tình hình trên, để bảo đảm an ninh mạng, Trung tâm Công nghệ thông tin đề nghị các đơn vị có hệ thống thông tin trực thuộc Bộ chủ động thực hiện các biện pháp sau:

- Tổ chức kiểm tra, rà soát các thiết bị DrayTek 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).*

- Tăng cường giám sát an ninh mạng, kịp thời phát hiện hoạt động tấn công mạng, phối hợp với Trung tâm Công nghệ thông tin trong điều tra, xác minh, xử lý đối tượng thực hiện tấn công mạng.

- Kết quả kiểm tra, rà soát đề nghị trao đổi bằng văn bản gửi về Trung tâm Công nghệ thông tin, địa chỉ: 113 Trần Duy Hưng, Cầu Giấy, Hà Nội trước ngày 24/11/2020.

Trong trường hợp cần thiết có thể liên hệ đầu mối hỗ trợ của Trung tâm Công nghệ thông tin: Phòng Kỹ thuật hạ tầng, điện thoại 024.39439060, thư điện tử: phongktht@most.gov.vn.

Trân trọng./.

Nơi nhận:
- Như trên;
- Thứ trưởng Bùi Thế Duy (để biết);
- Lưu: VT, KTHT.

GIÁM ĐỐC

BỘ KHOA HỌC VÀ CÔNG NGHỆ
TRUNG TÂM CÔNG NGHỆ THÔNG TIN

Hà Quốc Trung

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

(Kèm theo Công văn số 336 /TTCNTT-KTHT ngày 10 /11/2020)

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 VigorSvvitch20P2280	< 2.3.2