BỘ TƯ PHÁP
CỤC CÔNG NGHỆ THÔNG TIN

Số: 537/CNTT-HTKT&ATTT
V/v cảnh báo nguy cơ tấn công có chủ đích (APT) vào các thiết bị DrayTek.

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

Hà Nội, ngày 25 tháng 11 năm 2020

Kính gửi: - Các đơn vị thuộc Bộ Tư pháp;
- Cục Thi hành án dân sự các tỉnh, thành phố trực thuộc Trung ương.

Hiện nay, tình hình an toàn an ninh thông tin trong nước đang có diễn biến phức tạp, các đơn vị chuyên trách về an toàn an ninh thông tin liên tục đưa ra các cảnh báo, khuyến nghị về công tác đảm bảo an toàn an ninh thông tin. Thời gian qua, các chuyên gia bảo mật đã phát hiện nhiều chiến dịch tấn công có chủ đích (APT) thông qua khai thác lỗ hổng bảo mật trên dòng thiết bị DrayTek như: một số thiết bị định tuyến và chuyển mạch có lỗ hổng bảo mật nghiệm trọng (mã lỗi CVE-2020-8515), ảnh hưởng trực tiếp đến công tác đảm bảo an toàn thông tin của các cơ quan, tổ chức, bộ, ban, ngành cụ thể như sau:

- Tin tặc khai thác thành công lỗ hổng bảo mật này có thể đạt quyền truy cập cao nhất (quyền root) vào thiết bị;
- 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.

Từ tình hình trên, để đảm an toàn thông tin và phòng tránh nguy cơ bị tấn công có chủ đích (APT), Cục Công nghệ thông tin đề nghị các đơn vị 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;
- Tăng cường, nâng cao ý thức, kịp thời phát hiện hoạt động tấn công mạng, phối hợp với Cục Công nghệ thông tin để xác minh, xử lý;

- Thường xuyên cập nhật thông tin về an toàn an ninh thông tin tại chuyên mục An toàn thông tin trên trang thông tin điện tử của Cục Công nghệ thông tin: http://cntt.moj.gov.vn *(phụ lục kèm theo).*

Thông tin liên hệ với đầu mối tiếp nhận, yêu cầu hỗ trợ:

Phòng Hạ tầng kỹ thuật và An toàn thông tin.

Điện thoại: 0243.62739717

Email: csht@moj.gov.vn

Xin cảm ơn sự quan tâm, phối hợp của Quý đơn vị./.

Nơi nhận:
- Như trên;
- Bộ trưởng (để b/c);
- Thứ trưởng Nguyễn Khánh Ngọc (để b/c);
- Lưu: VT.

CỤC TRƯỞNG

CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM
CỤC CÔNG NGHỆ THÔNG TIN
BỘ TƯ PHÁP

Nguyễn Tiến Dũng

Phụ lục

Danh sách thiết bị Draytek tồn lại lỗ hổng bảo mật CVE-2020-8515
(Kèm theo công văn số: 537/CNTT-HTKT&ATTT ngày 25 tháng 11 năm 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 VigorSwitch20P2280	< 2.3.2