ỦY BAN NHÂN DÂN **TỈNH ĐẮK LẮK**	**CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM** **Độc lập – Tự do – Hạnh phúc**
Số: 8474/UBND-KGVX V/v nguy cơ bảo mật từ các thiết bị mạng của hãng D-Link	*Đắk Lắk, ngày 26 tháng 10 năm 2017*

Kính gửi:

- Văn phòng Tỉnh ủy;
- Văn phòng Đoàn Đại biểu Quốc hội tỉnh;
- Văn phòng HĐND tỉnh;
- Văn phòng UBND tỉnh;
- Các Sở, ban, ngành và đoàn thể của tỉnh;
- UBND các huyện, Thị xã, Thành phố.

Ngày 02/10/2017 Bộ Công an đã có thông báo số 27/TB-BCA-A68 về việc cảnh báo nguy cơ bảo mật từ các thiết bị mạng của hãng D-Link. Hiện nay, sản phẩm của hãng D-Link được sử dụng tương đối phổ biến trong cơ quan nhà nước, các tổ chức, doanh nghiệp và kể cả ở các hộ gia đình. Tuy nhiên, sản phẩm của hãng D-Link có nhiều lỗ hổng bảo mật nghiêm trọng, những lỗ hổng được cài đặt sẵn từ khi xuất xưởng liên tục được các chuyên gia an ninh mạng phát hiện và công bố.

Theo thống kê, từ 2001 đến nay, có 114 lỗ hổng bảo mật trên các sản phẩm của hãng này được phát hiện và công bố, gần 50% trong số đó được phát hiện trong 03 năm trở lại đây, 36 lỗ hổng bảo mật (chiếm hơn 30%) được phát hiện chỉ trong 09 tháng đầu năm 2017. Mới đây, ngày 08/9/2017, 10 lỗ hổng bảo mật zero-day trên các thiết bị Wifi Router D-Link 850L đã được công bố, cho phép tin tặc chiếm quyền điều khiển thiết bị, cập nhật firmware cài mã độc, đánh cắp thông tin, triển khai nhiều kịch bản tấn công nguy hiểm khác vào hệ thống mạng. Các lỗ hổng này được tồn tại trên cả 02 phiên bản của thiết bị Wifi Router D-Link 850L là: "DIR-850L Rev. A" – phiên bản A sử dụng firmware Fw114wwb07_H2ab_Beta1 và "DIR-850L Rev. B" phiên bản B sử dụng firmware Fw208wwb02, bao gồm như sau:

- Thiếu cơ chế bảo vệ Firmware: Do không có cơ chế bảo vệ thành phần điều khiển, tin tặc có thể tải lên một bộ điều khiển độc hại mới. Firmware dành cho D-Link 850 RevA không có mật khẩu, D-Link 850L RevB được bảo vệ bởi mật khẩu được mã hóa cứng.

- Lỗ hổng XSS: Cả hai tính năng LAN và WAN của D-Link 850L RevA đều chứa lỗ hổng XSS, cho phép tin tặc thực hiện tấn công người dùng nhằm đánh cắp cookie.

- Lỗ hổng lấy mật khẩu quản trị và thêm người dùng toàn quyền truy cập vào bộ định tuyến thông qua giao thức của MyDLink.

- Giao thức đám mây yếu: Giao thức MyDLink hoạt động thông qua kênh TCP không được mã hóa.

- Truy cập backdoor.

- Khóa riêng tư được mã cứng trên firmware.

- Không có cơ chế kiểm tra xác thực.

- Quyền quản lý tệp tin yếu và lưu trữ thông tin đăng nhập dưới dạng văn bản rõ ràng.

- Các máy trạm nội bộ sử dụng DHCP có thể bị tấn công đưa mã độc vào chiếm quyền kiểm soát thiết bị.

- Lỗ hổng tấn công từ chối dịch vụ khiến bộ định tuyến bị treo.

Những phát hiện trên cho thấy các sản phẩm mạng hãng D-Link chưa có cơ chế bảo mật bảo đảm, nếu các thiết bị này đặt vào những phân đoạn mạng quan trọng, khi bị tấn công sẽ nguy cơ mất an toàn, an ninh thông tin mạng.

Trên cơ sở đó, UBND tỉnh yêu cầu các Cơ quan, đơn vị, địa phương cần triển khai một số nội dung sau đây:

1. Rà soát các thiết bị mạng đang sử dụng tại cơ quan, đơn vị mình. Nếu có thiết bị mạng của hãng D-Link thuộc 02 phiên bản trên thì cập nhật ngay firmware phiên bản đã vá lỗi cho các thiết bị D-Link còn tồn tại lỗ hổng bảo mật nghiêm trọng; loại bỏ các thiết bị mạng của hãng D-Link có lỗ hổng nếu chưa được cập nhật bản vá; có kế hoạch thay thế hoặc chuyển các thiết bị D-Link ra khỏi các phân đoạn mạng quan trọng.

2. Đối với các hệ thống mạng quan trọng, chứa bí mật nhà nước, các cơ quan chủ quản cần phối hợp chặt chẽ với lực lượng An ninh mạng Bộ Công an để kiểm tra, rà soát an toàn, an ninh thông tin trước khi đưa thiết bị vào vận hành trong hệ thống.

Trên đây là cảnh báo nguy cơ lỗ hổng bảo mật gây mất an toàn, an ninh thông tin từ các thiết bị mạng của hãng D-Link. UBND tỉnh yêu cầu Thủ trưởng các cơ quan, đơn vị nghiêm túc triển khai thực hiện.

Đề nghị Văn phòng Tỉnh ủy triển khai văn bản này đến các Cơ quan, đơn vị trong khối Đảng./.

Nơi nhận:
- Như trên;
- CT, PCT UBND tỉnh;
- Văn phòng UBND tỉnh:
  + CVP, PCVP (Đ/c Nguyên);
  + Phòng QTTV, TTTT Công báo;
- Lưu VT, KGVX (H[T]N-90b)

KT. CHỦ TỊCH
PHÓ CHỦ TỊCH

Nguyễn Tuấn Hà