UBND TỈNH AN GIANG
SỞ NÔNG NGHIỆP VÀ PTNT

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

Số: 1714/SNNPTNT-KHCNMT
V/v cảnh báo các lỗ hổng bảo mật trong các sản phẩm Microsoft và trong BIOS của máy tính, thiết bị Dell

An Giang, ngày 04 tháng 8 năm 2021

Kính gửi:
- Các phòng thuộc Sở;
- Các đơn vị trực thuộc Sở.

Căn cứ Công văn số 692/CV-ĐƯCKCSCATTTM ngày 02/7/2021 về việc dự báo sớm nguy cơ tấn công mạng trên diện rộng và 04 lỗ hổng mới trong BIOS của máy tính, thiết bị Dell; và Công văn số 814/CV-ĐƯCKCSCATTTM ngày 26/7/2021 về việc 05 lỗ hổng bảo mật mức cao và nghiêm trọng trong các sản phẩm Microsoft của Đội ứng cứu khẩn cấp sự cố an toàn thông tin mạng.

Theo đó, trên cơ sở thực tế triển khai công tác giám sát an toàn thông tin và theo phân tích, đánh giá từ Trung tâm Giám sát an toàn không gian mạng quốc gia, Cục An toàn thông tin, Bộ Thông tin và Truyền thông dự báo một số lỗ hổng bảo mật có thể được tận dụng tiến hành chiến dịch tấn công mạng, cụ thể như sau:

- Lỗ hổng bảo mật **CVE-2021-1675** có mức độ nguy hiểm cao (7.8/10) ảnh hưởng đến hầu hết các phiên bản của hệ điều hành Windows bao gồm: Windows 10/8.1/7, Windows Server 2019/2016/2012/2008 và lỗ hổng này hoàn toàn có thể được tận dụng để tiến hành các chiến dịch tấn công có chủ đích APT lớn trên quy mô rộng trong thời gian ngắn sắp tới vào không gian mạng Việt Nam.

- 04 điểm yếu, lỗ hổng bảo mật mới **CVE-2021-21571, CVE-2021-21572, CVE-2021-21573, CVE-2021-21574** trong tính năng BIOSConnect và HTTPS Boot (tính năng, công cụ có sẵn trên hầu hết các máy tính, thiết bị của Dell để hỗ trợ việc cập nhật firmware và khôi phục hệ điều hành từ xa) trên BIOS của các máy tính, thiết bị hãng Dell. Đây là những lỗ hổng có phạm vi ảnh hưởng tương đối lớn, ảnh hưởng đến khoảng 30 triệu thiết bị tương ứng với 129 dòng máy tính xách tay, máy tính bảng và máy tính bàn. Đặc biệt 04 lỗ hổng này có thể kết hợp với nhau trong các chiến dịch tấn công có chủ đích để tấn công, kiểm soát máy tính, thiết bị của người dùng, từ đó tấn công sâu hơn vào các hệ thống thông tin quan trọng khác.

- 02 lỗ hổng **CVE-2021-34473, CVE-2021-34523**: tồn tại trong Microsoft Exchange Server, cho phép đối tượng tấn công có thể thực thi mã từ xa, nâng cao đặc quyền trên máy chủ thư điện tử.

- Lỗ hổng **CVE-2021-34527**: thực thi mã từ xa thứ 2 trong Windows Print Spooler (liên quan đến lỗ hổng CVE-2021-1675 trước đó). 02 lỗ hổng này đang được gọi với tên "PrinterNightmare".

- Lỗ hổng **CVE-2021-33781**: lỗ hổng cho phép đối tượng có đặc quyền thấp tấn công từ xa vượt qua các cơ chế kiểm tra bảo mật trong dịch vụ Active Directory để đạt được các đặc quyền cao hơn trên máy mục tiêu.

- Lỗ hổng **CVE-2021-34492**: lỗ hổng cho phép đối tượng tấn công vượt qua cơ chế kiểm tra trong Windows Certificate để giả mạo chứng chỉ. Lỗ hổng này là hoàn toàn có thể được dùng trong các cuộc tấn công khác nhau nhằm vào người dùng.

Nhằm đảm bảo an toàn cho hệ thống thông tin của các đơn vị, phòng tránh nguy cơ tấn công từ các lỗ hổng bảo mật nói trên, Sở Nông nghiệp và Phát triển nông thôn đề nghị các phòng và đơn vị trực thuộc thực hiện một số nội dung sau:

1. Kiểm tra, rà soát và xác định máy chủ, máy trạm sử dụng hệ điều hành Windows có khả năng bị ảnh hưởng. Định kỳ thực hiện cập nhật hệ điều hành, đồng thời thực hiện cập nhật bản vá bảo mật cho các máy bị ảnh hưởng, cụ thể:

- Lỗ hổng bảo mật **CVE-2021-1675**: Cập nhật bản vá bảo mật theo hướng dẫn tại ***Phụ lục 01*** đính kèm.

- Các lỗ hổng bảo mật **CVE-2021-34527, CVE-2021-33781, CVE-2021-34492**: Cập nhật các bản vá bảo mật theo hướng dẫn tại ***Phục lục 02*** đính kèm.

2. Đối với thiết bị Dell, thực hiện kiểm tra, rà soát thiết bị có khả năng bị ảnh hưởng bởi lỗ hổng trên để có phương án xử lý, khắc phục lỗ hổng. Cập nhật bản vá tương ứng theo phát hành của hãng. Trong trường hợp chưa có bản vá cần có phương án để ngăn chặn việc khai thác lỗ hổng đồng thời theo dõi thường xuyên thông tin về lỗ hổng để cập nhật ngay khi có bản vá. Hướng dẫn cập nhật khắc phục chi tiết tại ***Phụ lục 03*** đính kèm.

3. Tăng cường giám sát và thường xuyên theo dõi kênh cảnh báo của các cơ quan chức năng và các tổ chức lớn về an toàn thông tin để phát hiện kịp thời các nguy cơ tấn công mạng.

4. Báo cáo kết quả thực hiện tại phòng, ban, đơn vị về Sở Nông nghiệp và Phát triển nông thôn thông qua qua hệ thống quản lý văn bản chỉ đạo điều hành

VNPT iOffice và địa chỉ thư điện tử lhanh02@angiang.gov.vn trước ngày ***14/8/2021*** để tổng hợp báo cáo theo hạn định.

Trong quá trình thực hiện, nếu có vướng mắc vui lòng liên hệ Phòng Khoa học, Công nghệ và Môi trường (điện thoại: 02963.859.644) hoặc Lý Hoài Anh (di động: 0385.141.021) để được hướng dẫn, hỗ trợ.

Sở Nông nghiệp và Phát triển nông thôn đề nghị lãnh đạo các phòng và đơn vị trực thuộc quan tâm triển khai thực hiện./.

Nơi nhận:
- Như trên;
- Lưu: VT, PKHCNMT.LHA.

KT. GIÁM ĐỐC
PHÓ GIÁM ĐỐC

CỘNG HÒA X.H.C.N VIỆT NAM
SỞ NÔNG NGHIỆP VÀ PHÁT TRIỂN NÔNG THÔN
TỈNH AN GIANG

Trương Kiến Thọ