.UBND TỈNH HÒA BÌNH
SỞ THÔNG TIN VÀ TRUYỀN THÔNG

Số: 1048 /STTTT-CNTT
V/v cảnh báo 10 lỗ hổng bảo mật mức cao và nghiêm trọng trong các sản phẩm Microsoft

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

Hoà Bình, ngày 17 tháng 08 năm 2021

Kính gửi:
- Các Cơ quan Đảng, Đoàn thể tỉnh;
- Các Văn phòng: Tỉnh ủy, Đoàn ĐBQH và HĐND tỉnh, Ủy ban nhân dân tỉnh;
- Các Sở, ban, ngành;
- Các cơ quan, đơn vị sự nghiệp tỉnh;
- UBND các huyện, thành phố.

Căn cứ Công văn số 1115/CATTT-NCSC ngày 13/8/2021 của Cục An toàn thông tin - Bộ Thông tin và Truyền thông về việc 10 lỗ hổng bảo mật mức cao và nghiêm trọng trong các sản phẩm Microsoft *(bản điện tử kèm theo)*.

Ngày 10/8/2021 vừa qua, Microsoft phát hành danh sách bản vá lỗi tháng 8/2021 với 44 bản vá cho các lỗ hổng bảo mật trong sản phẩm của mình, 13 trong số 44 lỗ hổng được công bố lần này là lỗ hổng bảo mật cho phép thực thi mã từ xa, 7 lỗ hổng trong số này được đánh giá là quan trọng. Trong đó, đáng chú ý là 10 lỗ hổng bảo mật có mức ảnh hưởng tương đối lớn trong các sản phẩm Microsoft, đặc biệt là 04 lỗ hổng bảo mật tồn tại trong Windows Print Spooler và Microsoft Windows. Cụ thể như sau:

- 03 lỗ hổng bảo mật CVE-2021-36936, CVE-2021-36947, CVE-2021-34483 trong Windows Print Spooler cho phép đối tượng tấn công thực thi mã từ xa, nâng cao đặc quyền. Trong 2 tháng vừa qua, lỗ hổng trong Print Spooler đã có ảnh hưởng khá lớn và được quan tâm đặc biệt khi mà Microsoft liên tục công bố bản vá cho các lỗ hổng liên quan, bắt đầu với CVE-2021-1675 vào tháng 6, tiếp theo là bản vá lỗi cho CVE-2021-34527, còn được gọi là PrintNightmare vào tháng 7. Công cụ để khai thác các lỗ hổng trên đã được công bố rộng rãi trên Internet nên nguy cơ bị khai thác bởi các nhóm tấn công có chủ đích hoặc được sử dụng trong các cuộc tấn công diện rộng là rất lớn.

- Lỗ hổng bảo mật CVE-2021-26424 trong Microsoft Windows là lỗ hổng TCP/IP, cho phép đối tượng tấn công thực thi mã từ xa. Lỗ hổng này ảnh hưởng đến Windows 7 đến 10 và Windows Server 2008 đến 2019 với điểm CVSS 9.9 (nghiêm trọng). Tuy vậy, theo dự đoán của Trung tâm Giám sát An toàn không gian mạng quốc gia (NCSC), mã khai thác của lỗ hổng này sẽ khó được công bố sớm, do việc phát triển mã khai thác phải vượt qua các tính năng bảo vệ trong các phiên bản mới của Windows.

Nhằm đảm bảo an toàn an ninh thông tin cho các hệ thống thông tin của tỉnh, góp phần bảo đảm an toàn cho không gian mạng Việt Nam, Sở Thông tin và Truyền thông đề nghị các cơ quan, đơn vị khẩn trương thực hiện một số nội dung như 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. Thực hiện cập nhật bản vá bảo mật cho các máy bị ảnh hưởng theo hướng dẫn của Microsoft *(hướng dẫn chi tiết tham khảo tài liệu kèm theo Công văn số 1115/CATTT-NCSC ngày 13/8/2021 của Cục An toàn thông tin)*.

2. Tăng cường giám sát và sẵn sàng phương án xử lý khi phát hiện có dấu hiệu bị khai thác, tấn công mạng; đồng thời 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.

Trong trường hợp cần hỗ trợ, Quý đơn vị liên hệ đầu mối Trung tâm Giám sát an toàn không gian mạng quốc gia (NCSC) - Cục An toàn thông tin, điện thoại: 024.32091616, thư điện tử: ais@mic.gov.vn hoặc Phòng Công nghệ thông tin - Sở Thông tin và Truyền thông, điện thoại 0218.3857668.

Sở Thông tin và Truyền thông đề nghị các cơ quan, đơn vị triển khai thực hiện./.

Nơi nhận:
- Như trên;
- Cục ATTT-Bộ TTTT (p/h);
- Lãnh đạo Sở;
- Đội ƯCSC ATTTM tỉnh;
- Lưu VT, CNTT (Lo.60b).

GIÁM ĐỐC

Bùi Đức Nam