

Số: 2879 /STTTT-CNTT
V/v lỗ hổng bảo mật CVE-2021-40444
trong Microsoft Windows

Đồng Nai, ngày 4 tháng 10 năm 2021

Kính gửi:

- Các cơ quan đảng, nhà nước trên địa bàn tỉnh;
- Các tổ chức chính trị - xã hội thuộc địa bàn tỉnh.

Sở Thông tin và Truyền thông nhận được văn bản 1229/CATTT-NCSC ngày 10/9/2021 của Cục An toàn thông tin về việc lỗ hổng bảo mật CVE-2021-40444 trong Microsoft Windows.

Ngày 7/9/2021 vừa qua, Microsoft vừa công bố lỗ hổng bảo mật CVE2021-40444 trong Microsoft Windows, ảnh hưởng đến các phiên bản Windows 7/8/8.1RT/10, Windows Server 2008/2012/2016/2019/2022. Lỗ hổng này có điểm CVSS: 8.8 (cao), cho phép đối tượng tấn công thực thi mã từ xa trong MSHTML. MSHTML là một thành phần của hệ điều hành được dùng bởi khá nhiều chương trình của Microsoft như: Microsoft Office, bao gồm Word và PowerPoint,....

Hiện tại, lỗ hổng bảo mật này đã có mã khai thác công khai trên Internet, có thể dùng với nhiều kịch bản tấn công vào người dùng khác nhau với khả năng thành công rất cao. Vì vậy, Trung tâm Giám sát an toàn không gian mạng quốc gia (NCSC), Cục An toàn thông tin nhận thấy mức độ ảnh hưởng của lỗ hổng này khá lớn, có nguy cơ tấn công trên diện rộng và là mục tiêu nhằm đến của các đối tượng tấn công mạng có chủ đích (APT).

Nhằm đảm bảo an toàn thông tin cho hệ thống thông tin của Quý đơn vị, góp phần bảo đảm an toàn cho không gian mạng Việt Nam, Sở Thông tin và Truyền thông khuyến nghị Quý đơn vị thực hiện:

1. Kiểm tra, rà soát và xác định các máy sử dụng hệ điều hành Windows có khả năng bị ảnh hưởng. Tại thời điểm hiện tại chưa có thông tin bản vá cho lỗ hổng bảo mật trên, vì vậy để giảm thiểu nguy cơ tấn công, Quý đơn vị thực hiện biện pháp khắc phục theo hướng dẫn của Microsoft (chi tiết tham khảo tại phụ lục kèm theo).

2. Tăng cường các công cụ bảo vệ, công cụ giám sát, phần mềm phòng chống mã độc cho toàn bộ máy tính của người dùng. Hiện nay, công cụ Microsoft Defender Antivirus và Microsoft Defender for Endpoint đều có khả năng phát hiện và ngăn chặn lỗ hổng này.

3. 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 thiết có thể liên hệ đầu mối hỗ trợ của Cục An toàn thông tin: 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 Viễn thông - Sở Thông tin và Truyền thông, số điện thoại: 0251.8825678.

Trân trọng./.

Đính kèm: Văn bản 1229/CATTT-NCSC ngày 10/9/2021 của Cục An toàn thông tin về việc lỗ hổng bảo mật CVE-2021-40444 trong Microsoft Windows.

(Văn bản 1229/CATTT-NCSC tải về tại mục an toàn thông tin mạng theo địa chỉ <http://sttt.dongnai.gov.vn/Pages/news.aspx?CatId=56>).

Nơi nhận:

- Như trên;
- Giám đốc và PGĐ Sở;
- Trung tâm CNTT&TT;
- Lưu: VT, CNTTVT, TienLHV.

**KT. GIÁM ĐỐC
PHÓ GIÁM ĐỐC**

Võ Hoàng Khai