UBND TỈNH ĐỒNG NAI
SỞ Y TẾ

Số: 9400 /SYT-VP
V/v triển khai Công văn số 3140/STTTT-CNTTVT ngày 02/11/2021 của Sở Thông tin và Truyền thông.

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

Đồng Nai, ngày 08 tháng 11 năm 2021

Kính gửi: Giám đốc, Thủ trưởng các đơn vị trực thuộc.

Sở Y tế nhận được Công văn số 3140/STTTT-CNTTVT ngày 02/11/2021 của Sở Thông tin và Truyền thông về việc lỗ hổng bảo mật ảnh hưởng cao và nghiêm trọng trong các sản phẩm Microsoft (*đính kèm Công văn*).

Giám đốc Sở Y tế đề nghị Giám đốc, Thủ trưởng các đơn vị trực thuộc chỉ đạo các tổ chức, cá nhân phụ trách về công nghệ thông tin của đơn vị tổ chức triển khai thực hiện nội dung Công văn số 3140/STTTT-CNTTVT ngày 02/11/2021 của Sở Thông tin và Truyền thông.

Đề nghị Giám đốc, Thủ trưởng các đơn vị trực thuộc triển khai thực hiện theo sự chỉ đạo./.

Nơi nhận:
- Như trên;
- Lưu: VT,VP.

GIÁM ĐỐC

CỘNG HÒA X.H.C.N VIỆT NAM
SỞ Y TẾ
TỈNH ĐỒNG NAI

Phan Huy Anh Vũ

Số 2 - Phan Đình Phùng, phường Quang Vinh, thành phố Biên Hoà, tỉnh Đồng Nai
ĐT: (02513) 942641, Fax: (02513) 847269, Email: syt@dongnai.gov.vn, Website: syt.dongnai.gov.vn

UBND TỈNH ĐỒNG NAI
SỞ THÔNG TIN VÀ TRUYỀN THÔNG

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

Số: 3140 /STTTT-CNTTVT
V/v lỗ hổng bảo mật ảnh hưởng cao và nghiêm trọng trong các sản phẩm Microsoft

Đồng Nai, ngày 2 tháng 11 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 1411/CATTT-NCSC ngày 14/10/2021 của Cục An toàn thông tin về việc lỗ hổng bảo mật ảnh hưởng cao và nghiêm trọng trong các sản phẩm Microsoft.

- Lỗ hổng bảo mật CVE-2021-26427 trong Microsoft Exchange Server: Lỗ hổng này được coi là ít có khả năng bị khai thác, nhưng vẫn có thể cho phép đối tượng tấn công thực thi mã từ xa trên máy chủ mục tiêu. Điều này cho thấy, Exchange Server vẫn là mục tiêu hàng đầu của các nhóm tấn công có chủ đích (APT) từ tháng 3/2021 đến nay và có nhiều cách khai thác mà kẻ tấn công có thể tận dụng. Trung tâm Giám sát an toàn không gian mạng quốc gia (NCSC), Cục An toàn thông tin cũng đã đặc biệt nhấn mạnh tầm ảnh hưởng của Exchange Server thông qua nhiều văn bản cảnh báo rộng rãi về các lỗ hổng bảo mật trong Exchange Server trước đây.

- Lỗ hổng bảo mật CVE-2021-40486 trong Microsoft Word: Lỗ hổng có điểm CVSS: 7.8 (cao) cho phép đối tượng tấn công thực thi mã từ xa mà không cần xác thực, từ đó có thể hoàn toàn chiếm quyền truy cập hệ thống mục tiêu.

- Lỗ hổng bảo mật CVE-2021-40469 trong Windows DNS Server: Lỗ hổng có điểm CVSS: 7.8 (cao), ảnh hưởng đến các phiên bản khác nhau của Windows 7/8.1/10. Để khai thác lỗ hổng này, đối tượng tấn công cần xác thực để thực thi mã từ xa. - 05 lỗ hổng bảo mật (CVE-2021-40471, CVE-2021-40473, CVE-2021-40474, CVE-2021-40479, CVE-2021-40485) trong Microsoft Excel: có điểm CVSS: 7.8 (cao), cho phép đối tượng tấn công thực thi mã từ xa.

- Lỗ hổng bảo mật CVE-2021-40465 trong Windows Text Shaping: Lỗ hổng có điểm CVSS: 7.8 (cao) cho phép đối tượng tấn công thực thi mã từ xa mà không cần xác thực.

- Lỗ hổng bảo mật CVE-2021-41342 trong Windows MSHTML: Lỗ hổng có điểm CVSS: 6.8 (cao) cho phép đối tượng tấn công thực thi mã từ xa.

Số 01, đường 30/4, phường Thanh Bình, TP Biên Hòa, tỉnh Đồng Nai
TEL: (0251) 8825678 – Website: http://stttt.dongnai.gov.vn

- Lỗ hổng bảo mật CVE-2021-36970 trong Windows Print Spooler: Lỗ hổng có điểm CVSS: 8.8 (cao) cho phép đối tượng tấn công thực hiện tấn công giả mạo.

- 02 lỗ hổng bảo mật (CVE-2021-40461 và CVE-2021-38672) trong Windows Hyper-V: Các lỗ hổng này cho phép đối tượng tấn công thực thi mã từ xa, gây lỗi cấp phát bộ nhớ từ đó có thể đọc bộ nhớ trong của máy chủ.

Nhằm đảm bảo an toàn thông tin cho hệ thống thông tin của Quý đơn vị, góp phần bảo đảm bảo 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, xác định máy sử dụng hệ điều hành Windows có khả năng bị ảnh hưởng. Thực hiện cập nhật bản vá kịp thời để tránh nguy cơ bị tấn công (tham khảo thông tin tại phụ lục kèm theo).

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 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 1411/CATTT-NCSC ngày 14/10/2021 của Cục An toàn thông tin về việc lỗ hổng bảo mật ảnh hưởng cao và nghiêm trọng trong các sản phẩm Microsoft.

(Văn bản 1411/CATTT-NCSC tải về tại mục an toàn thông tin mạng theo địa chỉ http://stttt.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

CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM
SỞ THÔNG TIN VÀ TRUYỀN THÔNG
TỈNH ĐỒNG NAI

Võ Hoàng Khai