UBND TỈNH HƯNG YÊN
SỞ GIÁO DỤC VÀ ĐÀO TẠO

Số: 1774/SGDĐT-VP
V/v 19 lỗ hổng bảo mật mới trong VMware

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

Hưng Yên, ngày 27 tháng 9 năm 2021

Kính gửi:
- Các đơn vị giáo dục trực thuộc;
- Phòng GDĐT các huyện/thị xã/thành phố;
- Trung tâm GDNN – GDTX các huyện/thị xã/thành phố;

Căn cứ Công văn số 1069/STTTT-BCVTCNTT ngày 24/9/2021 của Sở Thông tin và Truyền thông Hưng Yên v/v 19 lỗ hổng bảo mật mới trong Vware,

Theo thông báo của Cục An toàn thông tin – Bộ Thông tin và Truyền thông về 19 lỗ hổng bảo mật mới trong Vware ảnh hưởng đến VMware vCenter Server phiên bản 7.0/6.7/6.5 và VMware vClound Foundation phiên bản 4.3.1/3.10.2.2. Trong đó đáng chú ý:

- Lỗ hổng bảo mật (CVE-2021-22005) có mức ảnh hưởng nghiêm trọng (điểm CVSS:9.8), cho phép đối tượng tấn công không cần xác thực có thể thực thi mã tùy ý.

- 11 lỗ hổng bảo mật (CVE-2021-21991, CVE-2021-22006, CVE-2021-22011, CVE-2021-22015, CVE-2021-22012, CVE-2021-22013, CVE-2021-22016, CVE-2021-22017, CVE-2021-22014, CVE-2021-22018, CVE-2021-21992) có mức ảnh hưởng cao, cho phép đối tượng tấn công khai thác dưới nhiều hình thức khác nhau như thu thập thông tin, tấn công leo thang, tấn công từ chối dịch vụ,... Trong đó có 07 lỗ hổng bảo mật (CVE-2021-22006, CVE-2021-22011, CVE-2021-22012, CVE-2021-22013, CVE-2021-22016, CVE-2021-22017, CVE-2021-22018) có thể khai thác mà không cần xác thực.

Để đảm bảo an toàn thông tin cho hệ thống thông tin dùng chung của tỉnh và của các cơ quan, đơn vị trên địa bàn tỉnh, góp phần bảo đảm an toàn cho không gian mạng Việt Nam, Sở Giáo dục và Đào tạo đề nghị đơn vị, trường học chỉ đạo bộ phận chuyên môn thực hiện rà soát, khắc phục lỗ hổng bảo mật trên theo khuyến nghị sau:

1. Thực hiện kiểm tra, rà soát và xác minh hệ thống thông tin có khả năng bị ảnh hưởng bởi lỗ hổng trên để có phương án xử lý, khắc phục lỗ hổng, thực hiện cập nhật bản vá phù hợp với phiên bản sản phẩm VMware đang sử dụng *(tham khảo hướng dẫn kèm theo Công văn số 1286/CATTT-NCSC gửi kèm).*

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

3. Trong trường hợp cần thiết cần hỗ trợ Quý cơ quan liên hệ đầu mối hỗ trợ của Cục An toàn thông tin: Trung tâm Giám sát an toàn không gian mạng quốc gia (NCSC), điện thoại 02432091616, thư điện tử: ais@mic.gov.vn.

Sở Giáo dục và Đào tạo đề nghị các đơn vị, trường học quan tâm chỉ đạo và phối hợp tổ chức thực hiện./.

Nơi nhận:
- Như trên;
- Ban Giám đốc;
- Các phòng thuộc Sở;
- Lưu: VT, VP.

KT. GIÁM ĐỐC
PHÓ GIÁM ĐỐC

CỘNG HÒA XH CHỦ NGHĨA VIỆT NAM
SỞ GIÁO DỤC VÀ ĐÀO TẠO
TỈNH HƯNG YÊN

Đỗ Văn Khải