UBND TỈNH ĐIỆN BIÊN
SỞ GIÁO DỤC VÀ ĐÀO TẠO

Số 2019 /SGDĐT-QLCL
V/v cảnh báo lỗ hổng bảo mật ảnh hưởng cao trong các sản phẩm Microsoft tháng 8/2022

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

Điện Biên, ngày22 tháng 8 năm 2022

Kính gửi:
- Phòng Giáo dục và Đào tạo các huyện, thị xã, thành phố;
- Các đơn vị trực thuộc Sở Giáo dục và Đào tạo;
- Các phòng CMNV Sở Giáo dục và Đào tạo;
- Các trung tâm GDNN-GDTX cấp huyện.

Căn cứ Văn bản số 1221/CATTT-NCSC ngày 10/8/2022 của Cục An toàn thông tin, về lỗ hổng bảo mật ảnh hưởng cao trong các sản phẩm Microsoft công bố tháng 8/2022.

Qua công tác theo dõi, giám sát trên không gian mạng, Trung tâm Giám sát an toàn không gian mạng quốc gia (NCSC), Cục An toàn thông tin - Bộ Thông tin và Truyền thông cảnh báo:

Ngày 09/8/2022, Microsoft đã phát hành danh sách bản vá tháng 8/2022 với 121 lỗ hổng bảo mật trong các sản phẩm của mình. Bản phát hành tháng này đặc biệt đáng chú ý các lỗ hổng bảo mật có mức ảnh hưởng cao, cụ thể sau:

- Lỗ hổng bảo mật CVE-2022-34713 trong Microsoft Windows Support Diagnostic Tool (MSDT) cho phép đối tượng tấn công thực thi mã từ xa. Lỗ hổng này đang được khai thác rộng rãi trên Internet.

- 04 lỗ hổng bảo mật CVE-2022-21980, CVE-2022-24477, CVE-2022-24516, CVE-2022-30134 trong Microsoft Exchange Server cho phép đối tượng tấn công thu thập thông tin và thực hiện leo thang đặc quyền.

- Lỗ hổng bảo mật CVE-2022-35804 trong SMB Client and Server cho phép đối tượng tấn công thực thi mã từ xa trên phiên bản Windows 11.

- Lỗ hổng bảo mật CVE-2022-34715 trong Windows Network File System cho phép đối tượng tấn công chưa xác thực có thể thực thi mã từ xa.

- Lỗ hổng bảo mật CVE-2022-35742 trong Microsoft Outlook cho phép đối tượng tấn công thực hiện tấn công từ chối dịch vụ.

Nhằm đảm bảo an toàn thông tin cho hệ thống của các cơ quan, đơn vị, góp phần bảo đảm an toàn cho không gian mạng của tỉnh, Sở Giáo dục và Đào tạo yêu cầu các đơn vị triển khai thực hiện ngay một số nội dung sau:

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 *(danh sách lỗ hổng và hướng dẫn chi tiết tham khảo tại phụ lục kèm theo).*

2. Tăng cường theo dõi giám sát hệ thống và có phương án xử lý khi phát hiện có dấu hiệu bị khai thác, tấn công mạng.

Khi xảy ra sự cố liên quan đến an toàn, an ninh thông tin mạng và các hệ thống thông tin khác, liên hệ ông Nguyễn Hùng Cường - Chuyên viên phòng KTKĐCLGD&CNTT, Sở Giáo dục và Đào tạo theo số điện thoại 0968199100 để được hỗ trợ.

Nhận được văn bản này, Sở Giáo dục và Đào tạo yêu cầu Thủ trưởng các đơn vị nghiêm túc triển khai thực hiện./.

Nơi nhận:
- Như trên;
- Lãnh đạo Sở GDĐT;
- Lưu: VT, QLCL.

KT.GIÁM ĐỐC
PHÓ GIÁM ĐỐC

CỘNG HÒA X.H.C.N VIỆT NAM
SỞ GIÁO DỤC VÀ ĐÀO TẠO
TỈNH ĐIỆN BIÊN

Cù Huy Hoàn

Ký bởi Sở Giáo dục và Đào tạo
Giờ ký: 2022-08-22T15:40:21.7362055+07:00
Tỉnh Điện Biên

Phụ lục: Thông tin lỗ hổng bảo mật

1. Thông tin lỗ hổng bảo mật

STT	CVE	Mô tả	Link tham khảo
1	CVE-2022-34713	- Điểm CVSS: 7.8 (Cao) - Lỗ hổng trong Microsoft Windows Support Diagnostic Tool (MSDT) cho phép đối tượng tấn công thực thi mã từ xa. - Ảnh hưởng: Windows 7/8.1/10/11, Windows Server 2008/2012.	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-34713
2	CVE-2022-21980 CVE-2022-24477 CVE-2022-24516 CVE-2022-30134	- Điểm CVSS: 8.0 (Cao) - Lỗ hổng trong Microsoft Exchange Server cho phép đối tượng tấn công thu thập thông tin và thực hiện leo thang đặc quyền. - Ảnh hưởng: Microsoft Exchange Server 2013/2016/2019.	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-21980 https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-24477 https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-24516 https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-30134
3	CVE-2022-35804	- Điểm CVSS: 8.8 (Cao) - Lỗ hổng trong SMB Client and Server cho phép đối tượng tấn công	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-35804
		chưa xác thực có thể thực thi mã từ xa. - Ảnh hưởng: Windows 11.	

4	CVE-2022-34715	- Điểm CVSS: 9.8 (Nghiêm trọng) - Lỗ hổng trong Windows Network File System cho phép đối tượng tấn công chưa xác thực có thể thực thi mã từ xa. - Ảnh hưởng: Windows	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-34715
5	CVE-2022-35742	- Điểm CVSS: 7.5 (Cao) - Lỗ hổng trong Microsoft Outlook cho phép đối tượng tấn công thực hiện tấn công từ chối dịch vụ. - Ảnh hưởng: Microsoft Outlook 2012/2016, Microsoft Office LTSC 2021/2019, Microsoft 365 Apps.	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-35742

2. Hướng dẫn khắc phục

Biện pháp tốt nhất để khắc phục là cập nhật bản vá cho các lỗ hổng bảo mật nói trên theo hướng dẫn của hãng. Đơn vị tham khảo các bản cập nhật phù hợp cho các sản phẩm đang sử dụng tại link nguồn tham khảo tại mục 1 của phụ lục.

3. Nguồn tham khảo

https://msrc.microsoft.com/update-guide/releaseNote/2022-Aug
https://www.zerodayinitiative.com/blog/2022/8/9/the-august-2022-security-update-review