UBND TỈNH ĐIỆN BIÊN
SỞ GIÁO DỤC VÀ ĐÀO TẠO

Số 2863 /SGDĐT-QLCL
V/v cảnh báo lỗ hổng bảo mật ảnh hưởng cao trong các sản phẩm của Microsoft tháng 11/2022

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

Điện Biên, ngày 17 tháng 11 năm 2022

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

Căn cứ Văn bản số 1824/CATTT-NCSC ngày 11/11/2022 của Cục An toàn thông tin về cảnh báo lỗ hổng bảo mật ảnh hưởng cao và nghiêm trọng trong sản phẩm Microsoft công bố tháng 11/2022 .

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 08/11/2022, Microsoft đã phát hành danh sách bản vá tháng 11/2022 với 64 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 và nghiêm trọng sau:

- 06 lỗ hổng bảo mật CVE-2022-41082, CVE-2022-41040, CVE-2022-41080, CVE-2022-41079, CVE-2022-41078, CVE-2022-41123 trong Microsoft Exchange Server cho phép đối tượng tấn công thực thi mã từ xa, nâng cao đặc quyền. Trong đó, 02 lỗ hổng CVE-2022-41082, CVE-2022-41040 đã được cảnh báo tại văn bản số 1484/CATTT-VNCERT/CC về việc cảnh báo lỗ hổng bảo mật zero-day ảnh hưởng nghiêm trọng đến Microsoft Exchange phát hành ngày 30/9/2022.

- 02 lỗ hổng bảo mật CVE-2022-41128, CVE-2022-41118 trong Windows Scripting Languages cho phép đối tượng tấn công thực thi mã từ xa. Lỗ hổng này đang bị khai thác trong thực tế.

- Lỗ hổng bảo mật CVE-2022-41091 trong Windows Mark of the Web cho phép đối tượng tấn công thực hiện tấn công vượt qua cơ chế bảo mật.

- Lỗ hổng bảo mật CVE-2022-41073 trong Windows Print Spooler cho phép đối tượng tấn công thực hiện tấn công nâng cao đặc quyền.

- Lỗ hổng bảo mật CVE-2022-41125 trong Windows CNG Key Insolation Service cho phép đối tượng tấn công thực hiện tấn công nâng cao đặc quyền.

- 03 lỗ hổng bảo mật CVE-2022-41044, CVE-2022-41088, CVE-2022-41039 trong Windows Point-to-Point cho phép đối tượng tấn công thực thi mã từ xa.

- 04 lỗ hổng bảo mật CVE-2022-41105, CVE-2022-41106, CVE-2022-

41063, CVE-2022-41104 trong Microsoft Excel cho phép đối tượng tấn công thực thi mã từ xa, tấn công giả mạo (Spoofing), thực hiện tấn công vượt qua cơ chế bảo mật.

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 KT-KĐCLGD&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: 2022-11-17T14:05:52.7717543+07:00
Tỉnh Điện Biên

PHỤ LỤC: THÔNG TIN LỖ HỔNG BẢO MẬT

1. Thông tin các lỗ hổng bảo mật

STT	CVE	Mô tả	Link tham khảo
1	CVE-2022-41082, CVE-2022-41040, CVE-2022-41080, CVE-2022-41079, CVE-2022-41078, CVE-2022-41123	- Điểm CVSS: 8.8 (Cao) -Lỗ hổng trong Microsoft Exchange Server cho phép đối tượng tấn công thực thi mã từ xa, nâng cao đặc quyền. - Ảnh hưởng: Microsoft Exchange Server 2016 CU 23/22, Exchange Server 2019 CU 11, Exchange Server 2013 CU 23	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-41082 https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-41040 https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-41080 https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-41123 https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-41078 https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-41079
2	CVE-2022-41128, CVE-2022-41118	- Điểm CVSS: 8.8 (Cao) - Lỗ hổng trong trong Windows Scripting Languages cho phép đối tượng tấn công thực thi mã từ xa. Lỗ hổng này đang bị khai thác trong thực tế. - Ảnh hưởng: Windows Server 2008/2012/2016/2019/2022 , Windows 11/10/8.1/7.	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-41128 https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-41118
3	CVE-2022-41091	- Điểm CVSS: 5.4 (Trung bình) -Lỗ hổng trong Windows Mark of the Web cho phép đối tượng tấn công thực hiện tấn công vượt qua cơ chế bảo mật. Ảnh hưởng: Windows 10/11, Windows Server 2016/2019/2022.	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-41091

4	CVE-2022-41073	- Điểm CVSS: 7.8 (Cao) -Lỗ hổng Windows Print Spooler cho phép đối tượng tấn công thực hiện tấn công nâng cao đặc quyền. - Ảnh hưởng: Windows Server 2008/2012/2016/2019/2022 , Windows 11/10/8.1/7.	https://msrc.microsoft.com /update-guide/vulnerability/CVE-2022-41073
5	CVE-2022-41125	- Điểm CVSS: 7.8 (Cao) -Lỗ hổng Windows CNG Key Insolation Service cho phép đối tượng tấn công thực hiện tấn công nâng cao đặc quyền. - Ảnh hưởng: Windows 8.1/10/11, Windows Server 2012/2016/2019/2022	https://msrc.microsoft.com /update-guide/vulnerability/CVE-2022-41125
6	CVE-2022-41044, CVE-2022-41088, CVE-2022-41039	- Điểm CVSS: 8.1 (Cao) -Lỗ hổng trong Windows Point-to-Point cho phép đối tượng tấn công thực thi mã từ xa. - Ảnh hưởng: Windows 8.1/10/11, Windows Server 2012/2016/2019.	https://msrc.microsoft.com /update-guide/vulnerability/CVE-2022-41044 https://msrc.microsoft.com /update-guide/vulnerability/CVE-2022-41088 https://msrc.microsoft.com /update-guide/vulnerability/CVE-2022-41039

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-Nov

https://www.zerodayinitiative.com/blog/2022/11/8/the-november-2022-security-update-review