UBND TỈNH ĐIỆN BIÊN
SỞ THÔNG TIN VÀ TRUYỀN THÔNG

Số: 2041 /STTTT-CNTT
V/v cảnh báo lỗ hổng bảo mật ảnh hưởng cao và nghiêm trọng trong các sản phẩm Microsoft công bố tháng 12/2021

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

Điện Biên, ngày 22 tháng 12 năm 2021

Kính gửi:
- Các Sở, ngành, đoàn thể tỉnh;
- UBND các huyện, thị xã, thành phố.

Căn cứ Văn bản số 1749/CATTT-NCSC ngày 15/12/2021 của Cục An toàn thông tin về lỗ hổng bảo mật ảnh hưởng cao và nghiêm trọng trong các sản phẩm Microsoft công bố tháng 12/2021.

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 14/12/2021, Microsoft đã phát hành danh sách bản vá tháng 12 với 67 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 cho phép đối tượng có thể thực hiện tấn công thực thi mã từ xa, nâng cao đặc quyền, xóa tệp tin trong hệ thống mục tiêu… mà không cần xác thực như sau:

- Lỗ hổng bảo mật CVE-2021-43907 trong Windows Sybsystem for Linux (WSL), cho phép đối tượng tấn công thực thi mã từ xa.

- Lỗ hổng bảo mật CVE-2021-43899 trong Microsoft 4K Wireless Display Adapter, cho phép đối tượng tấn công thực thi mã từ xa.

- Lỗ hổng bảo mật CVE-2021-43215 trong iSNS Server, cho phép đối tượng tấn công thực thi mã từ xa.

- Lỗ hổng bảo mật CVE-2021-43890 trong Windows AppX Installer, cho phép đối tượng tấn công thực hiện tấn công giả mạo. Bên cạnh đó, lỗ hổng này được cho là đang được khai thác trong chiến dịch tấn công mã độc Emotet, Trickbot, Bazaloader.

- Lỗ hổng bảo mật CVE-2021-42309 trong Microsoft SharePoint Server, cho phép đối tượng tấn công thực thi mã từ xa.

- Lỗ hổng bảo mật CVE-2021-41333 trong Windows Print Spooler, cho phép đối tượng tấn công thực hiện tấn công nâng cao đặc quyền.

- Lỗ hổng bảo mật CVE-2021-43880 trong Windows Mobile Device Management, cho phép đối tượng tấn công nâng cao đặc quyền, xóa tệp tin trong hệ thống mục tiêu.

- Lỗ hổng bảo mật CVE-2021-43893 trong Windows Encrypting File System (EFS), cho phép đối tượng tấn công nâng cao đặc quyền.

- Lỗ hổng bảo mật CVE-2021-43240 trong NTFS Set Short Name, cho phép đối tượng tấn công nâng cao đặc quyền.

- Lỗ hổng bảo mật CVE-2021-43883 trong Windows Installer cho phép đối tượng tấn công leo thang đặc quyền.

Nhằm đảm bảo an toàn thông tin cho hệ thống của các cơ quan, đơn vị trên địa bàn tỉnh, góp phần bảo đảm an toàn không gian mạng Việt Nam. Sở Thông tin và Truyền thông đề nghị các cơ quan, đơn vị phối hợp thực hiện một số nhiệm vụ sau:

1. Kiểm tra, rà soát và 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 *(hướng dẫn chi tiết tham khảo tại phụ lục 01 gửi 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.

3. Phối hợp với Trung tâm CNTT&TT - Sở Thông tin và Truyền thông kiểm tra, rà soát, kịp thời xử lý đối với các hệ thống hiện đang quản lý; bố trí bộ phận ứng cứu sự cố hỗ trợ các đơn vị khắc phục sự cố khi có yêu cầu.

Đầu mối hỗ trợ, ứng cứu an ninh mạng Sở Thông tin và Truyền thông: *Đ/c Mai Xuân Dũng-Phòng Công nghệ Thông tin, điện thoại: 0914.599.177; Đ/c Nguyễn Mạnh Cường - Trung tâm CNTT&TT, điện thoại: 3.826.288; điện thoại 0946.560.568.*

Trân trọng./.

Nơi nhận:
- Như trên;
- Công an tỉnh (p/h);
- Ban Giám đốc Sở;
- Trung tâm CNTT&TT;
- Lưu: VT, CNTT.

KT. GIÁM ĐỐC
PHÓ GIÁM ĐỐC

Phạm Thanh Nam

Phụ lục 01: **Thông tin lỗ hổng bảo mật**

(Kèm theo Công văn số /STTTT-CNTT ngày / 12 /2021 của Sở Thông tin và Truyền thông)

1. Thông tin lỗ hổng bảo mật

STT	CVE	Mô tả	Link tham khảo
1	CVE-2021-43890	- Điểm CVSS: 7.1 (cao) - Lỗ hổng trong Windows AppX Installer, cho phép đối tượng tấn công thực hiện tấn công giả mạo.	https://msrc.microsoft. com/update-guide/enUS/vulnerability/CVE2021-43890
2	CVE-2021-43907	- Điểm CVSS: 9.8 (Nghiêm trọng) - Lỗ hổng trong Windows Subsystem for Linux (WSL), cho phép đối tượng tấn công thực thi mã từ xa. - Ảnh hưởng: Visual Studio Code WLS Extension	https://msrc.microsoft. com/updateguide/vulnerability/CVE-2021-43907
3	CVE-2021-42309	- Điểm CVSS: 8.8 (Cao) - Lỗ hổng trong Microsoft SharePoint Server, cho phép đối tượng tấn công thực thi mã từ xa. - Ảnh hưởng: Microsoft SharePoint Foundation 2013, SharePoint Server 2019, SharePoint Enterprise Server 2016.	https://msrc.microsoft. com/updateguide/vulnerability/CVE-2021-42309
4	CVE-2021-43899	- Điểm CVSS: 9.8 (Nghiêm trọng) - Lỗ hổng trong Microsoft 4K Wireless Display Adapter, cho phép đối tượng tấn công thực thi mã từ xa. - Ảnh hưởng: Microsoft 4K Wireless Display Adapter	https://msrc.microsoft. com/update-guide/enUS/vulnerability/CVE2021-43899

5	CVE-2021-43215	- Điểm CVSS: 9.8 (Nghiêm trọng) - Lỗ hổng trong iSNS Server, cho phép đối tượng tấn công thực thi mã từ xa. - Ảnh hưởng: Windows Server 2008/2012/2016/2019, Windows 7/8.1/10.	https://msrc.microsoft. com/update-guide/vulnerability/CV E-2021-43215
6	CVE-2021-41333	- Điểm CVSS: 7.8 (cao) - Lỗ hổng trong Windows Print Spooler, cho phép đối tượng tấn công nâng cao đặc quyền. - Ảnh hưởng: Windows Server 2019/2016/2012/2008, Windows 8.1/7/10.	https://msrc.microsoft. com/updateguide/vulnerability/CV E-2021-41333
7	CVE-2021-43880	- Lỗ hổng trong Windows Mobile Device Management, cho phép đối tượng tấn công nâng cao đặc quyền. - Ảnh hưởng: Windows 11	https://msrc.microsoft. com/updateguide/vulnerability/CV E-2021-43880
8	CVE-2021-43893	- Điểm CVSS: 7.5 (cao) - Lỗ hổng trong Windows Encrypting File System (EFS) cho phép đối tượng tấn công nâng cao đặc quyền. - Ảnh hưởng: Windows 10/11, Windows Server 2022.	https://msrc.microsoft. com/updateguide/vulnerability/CV E-2021-43893
9	CVE-2021-43240	- Điểm CVSS: 7.8 (cao) - Lỗ hổng trong NTFS Set Short Name cho phép đối tượng tấn công nâng cao đặc quyền. - Ảnh hưởng: Windows	https://msrc.microsoft. com/updateguide/vulnerability/CV E-2021-43240

		10/11,	
10	CVE-2021-43883	Điểm CVSS: 7.8 (cao) - Lỗ hổng trong Windows Installer, cho phép đối tượng tấn công nâng cao đặc quyền. - Ảnh hưởng: Windows Server 2022/2019/2016/2012/2008, Windows 11/10/8.1/7	https://msrc.microsoft.com/updateguide/vulnerability/CVE-2021-43883

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. Các 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/en-us