UBND TỈNH ĐIỆN BIÊN
SỞ THÔNG TIN VÀ TRUYỀN THÔNG

Số: 1164 /STTTT-CNTT
V/v cảnh báo 10 lỗ hổng bảo mật mức cao và nghiêm trọng trong các sản phẩm Microsoft

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

Điện Biên, ngày 18 tháng 8 năm 2021

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

Căn cứ Văn bản số 1115/CATTT-NCSC ngày 13/08/2021 của Cục An toàn thông tin về 10 lỗ hổng bảo mật mức cao và nghiêm trọng trong các sản phẩm Microsoft.

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 đã cảnh báo: 10 lỗ hổng bảo mật có mức ảnh hưởng tương đối lớn trong các sản phẩm của Microsoft, đặc biệt 04 lỗ hổng bảo mật tồn tại trong Windows Print Spooler và Microsoft Windows gồm 03 lỗ hổng bảo mật **(CVE-2021-36936, CVE-2021-36947, CVE-2021-34483)** trong Windows Print Spooler cho phép đối tượng tấn công thực thi mã từ xa, nâng cao đặc quyền. 01 lỗ hổng bảo mật **(CVE-2021-26424)** trong Microsoft Windows là lỗ hổng ICP/IP, cho phép đối tượng tấn công thực thi mã từ xa, anh hưởng từ Windows 7 đến 10 và Windows Server 2008 đến 2019.

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 cho không gian mạng Việt Nam. Sở Thông tin và Truyền thông đề nghị các cơ quan, đơn vị phối hợp thực hiện:

1. Kiểm tra, rà soát và xác định máy chủ, máy trạm sử dụng hệ điều hành Windows có khả năng bị ảnh hưởng. Thực hiện cập nhật bản vá bảo mật cho các máy bị ảnh hưởng theo hướng dẫn *(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.

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.

Sở Thông tin và Truyền thông đề nghị các cơ quan, đơn vị khẩn trương phối hợp thực hiện.

Đầu mối hỗ trợ, ứng cứu sự cố an toàn 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: 3826288; 0946.560.568.

Trân trọng./.

Nơi nhận:
- Như trên;
- Ban Giám đốc Sở;
- Trung tâm CNTT&TT;
- Lưu: VT, CNTT.

KT. GIÁM ĐỐC
PHÓ GIÁM ĐỐC

CỘNG HOÀ XÃ HỘI CHỦ NGHĨA VIỆT NAM
SỞ THÔNG TIN VÀ TRUYỀN THÔNG
TỈNH ĐIỆN BIÊN

Phạm Thanh Nam

Phụ lục: Thông tin lỗ hổng bảo mật

(Kèm theo Công văn số 1164/STTTT-CNTT ngày 18 / 8 /2021 của Sở Thông tin và Truyền thông)

1. Thông tin lỗ hổng bảo mật

TT	CVE	Mã ta	Ghi chu
1	CVE-2021-36947	- Lỗ hổng tồn tại trong Windows Print Spooler, cho phép đối tượng tấn công thực thi mã từ xa. - Điểm CVSS: 8.8 (Cao) - Ảnh hưởng: Windows 7/8.1/10 va Windows Server 2008/2012/2019.	https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2021-36947
	CVE-2021-36936	- Lỗ hổng tồn tại trong Windows Print Spooler, cho phép đối tượng tấn công thực thi mã từ xa. - Điểm CVSS: 8.8 (Cao) - Ảnh hưởng: Windows 7/8.1/10 va Windows Server 2008/2012/2019.	https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2021-36936
	CVE-2021-34483	- Lỗ hổng tồn tại trong Windows Print Spooler, cho phép đối tượng tấn công nâng cao đặc quyền. - Điểm CVSS: 7.8 (Cao) - Ảnh hưởng: Windows 7/8.1/10 va Windows Server 2008/2012/2016.	https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2021-34483
2	CVE-2021-26424	- Lỗ hổng tồn tại liên quan đến giao thức TCP/IP của Windows, cho phép đối tượng tấn công thực thi mã từ xa. - Điểm CVSS: 9.9 (Nghiêm trọng) - Ảnh hưởng: Windows 7 den 10 va Windows Server 2008 den 2019.	https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2021-26424

3	CVE-2021-34535	- Lỗ hổng tồn tại trong Remote Desktop Client, cho phép đối tượng tấn công thực thi mã từ xa. - Điểm CVSS: 8.8 (Cao) - Ảnh hưởng: Windows 7/8.1/10 va Windows Server 2008/2012/2019.	https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2021-34535
4	CVE-2021-36948	- Lỗ hổng tồn tại trong Windows Update Medic Service (WaasMedic), cho phép đối tượng tấn công nâng cao đặc quyền. - Điểm CVSS: 7.8 (Cao) - Ảnh hưởng: Windows 10 va Windows Server 2019.	https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2021-36948
5	CVE-2021-36942	- Lỗ hổng tồn tại trong Windows Local Security Authority (LSA), cho phép đối tượng tấn công thực hiện tấn công giả mạo. - Điểm CVSS: 7.5 (Cao) - Ảnh hưởng: Windows 10 va Windows Server 2019.	https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2021-36942
6	CVE-2021-36941	- Lỗ hổng tồn tại trong Microsoft Word, cho phép đối tượng tấn công thực thi mã từ xa. - Điểm CVSS: 7.8 (Cao) - Ảnh hưởng: Microsoft 365, Microsoft Office 2019.	https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2021-36941
7	CVE-2021-34478	- Lỗ hổng tồn tại trong Microsoft Office, cho phép đối tượng tấn công thực thi mã từ xa. - Điểm CVSS: 7.8 (Cao) - Ảnh hưởng: Microsoft 365, Microsoft Office 2019.	https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2021-34478

8	CVE-2021-34524	- Lỗ hổng tồn tại trong Microsoft Dynamics 365 (on-premises), cho phép đối tượng tấn công thực thi mã từ xa. - Điểm CVSS: 8.1 (Cao) - Ảnh hưởng: Microsoft Dynamics 365 (on-premises) version 9.0 va 9.1	https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2021-34524
9	CVE-2021-26426	- Lỗ hổng tồn tại trong Windows User Profile Service cho phép đối tượng tấn công nâng cao đặc quyền. - Điểm CVSS: 7.8 (Cao) - Ảnh hưởng: Windows Server 2008/2012/2016/2019, Windows 7/8.1/10	https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2021-26426
10	CVE-2021-34484	- Lỗ hổng tồn tại trong Windows User Profile Service cho phép đối tượng tấn công nâng cao đặc quyền. - Điểm CVSS: 7.8 (Cao) - Ảnh hưởng: Windows Server 2008/2012/2016/2019, Windows 7/8.1/10	https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2021-34484

2. Hướng dẫn khắc phục

Biện pháp tốt nhất để khắc phục lỗ hổng bảo mật này là cập nhật bản vá. Trong trường hợp chưa thể cập nhật bản vá kịp thời, đơn vị thực hiện các biện pháp khắc phục theo hướng dẫn của hãng để giảm thiểu nguy cơ tấn công *(link hướng dẫn của hãng theo bảng trên).*