UBND TỈNH THANH HOÁ
SỞ TÀI NGUYÊN VÀ MÔI TRƯỜNG

Số: 7265 /STNMT - CNTT
V/v cảnh báo 10 lỗ hổng bảo mật mức cao và nghiêm trọng trong các sản phẩm Microsoft.

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

Thanh Hoá, ngày 26 tháng 8 năm 2021

Kính gửi: Trưởng các đơn vị thuộc Sở.

Sở Tài nguyên và Môi trường nhận được Công văn số 1727/STTTT-CNTT ngày 17/8/2021 của Sở Thông tin và Truyền thông về việc cảnh báo 10 lỗ hổng bảo mật mức cao và nghiêm trọng trong các sản phẩm Microsoft.

Qua phân tích và đánh giá từ Cục An toàn thông tin, Bộ Thông tin và Truyền thông đã ghi nhận 44 bản vá các điểm yếu, lỗ hổng bảo mật mới trên các sản phẩm của hãng Microsoft công bố trong tháng 8 năm 2021. Trong đó, đáng chú ý là 10 lỗ hổng bảo mật có mức ảnh hưởng cao và nghiêm trọng. Để tăng cường chủ động phòng ngừa các rủi ro mất an toàn thông tin tại hệ thống thông tin của Sở, Giám đốc Sở yêu cầu các đơn vị thuộc Sở khẩn trương triển khai một số nội dung sau:

1. Giao Trung tâm Công nghệ thông tin:

- Tăng cường theo dõi giám sát hệ thống đồng thời thường xuyên theo dõi kênh cảnh báo của các cơ quan chức năng và sẵn sàng phương án xử lý khi phát hiện có dấu hiệu bị khai thác, tấn công mạng; hỗ trợ các đơn vị khi có khó khăn vướng mắc.

- Đăng tải toàn bộ nội dung Công văn số 1727/STTTT-CNTT ngày 17/8/2021 của Sở Thông tin và Truyền thông trên Cổng thông tin điện tử Sở Tài nguyên và Môi trường Thanh Hóa.

2. Giao trưởng các đơn vị thuộc Sở:

- Phổ biến, quán triệt đến toàn thể công chức, viên chức và người lao động thuộc đơn vị mình thực hiện kiểm tra, rà soát và xác định các máy tính, máy chủ đang cài đặt các phần mềm, ứng dụng có khả năng bị ảnh hưởng bởi các lỗ hổng trên, liên hệ với Trung tâm Công nghệ thông tin để có phương án xử lý, khắc phục lỗ hổng. Cập nhật

phiên bản mới nhất theo khuyến nghị của hãng sản xuất để khắc phục các nguy cơ mất an toàn thông tin. *(Có phụ lục thông tin các lỗ hổng bảo mật kèm theo).*

Theo các nội dung trên, yêu cầu Trưởng các đơn vị quan tâm triển khai thực hiện./.

Nơi nhận:
- Như trên;
- Giám đốc Sở (để b/c);
- Lưu: VT, TTCNTT.

KT.GIÁM ĐỐC
PHÓ GIÁM ĐỐC

CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM
SỞ TÀI NGUYÊN VÀ MÔI TRƯỜNG
TỈNH THANH HÓA

Phùng Đình Ảnh

Phụ lục: Thông tin các lỗ hổng bảo mật

(*Kèm theo công văn số /STNMT-CNTT ngày tháng năm 2021 của Sở Tài nguyên và Môi trường***)**

Thông tin các lỗ hổng bảo mật

STT	CVE	Mô tả	Ghi chú
1.1	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 và Windows Server 2008/2012/2019.	https://msrc.microsoft.com/update-guide/enUS/vulnerability/CVE-2021-36947
1.2	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 và Windows Server 2008/2012/2019.	https://msrc.microsoft.com/update-guide/enUS/vulnerability/CVE-2021-36936
1.3	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 và Windows Server 2008/2012/2016.	https://msrc.microsoft.com/update-guide/enUS/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 đến 10 và Windows Server 2008 đến 2019.	https://msrc.microsoft.com/update-guide/enUS/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 và Windows Server 2008/2012/2019.	https://msrc.microsoft.com/update-guide/enUS/vulnerability/CVE-2021-34535
4	CVE-2021-36948	- Lỗ hổng tồn tại trong Windows Update MedicService (WaasMedic), cho phép đối tượng tấn công nâng cao đặc quyền. - Điểm CVSS: 7.8 (Cao) - Ảnh hưởng: Windows 10 và Windows Server 2019.	https://msrc.microsoft.com/update-guide/enUS/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 và	https://msrc.microsoft.com/update-guide/enUS/vulnerability/CVE-2021-36942

		Windows Server 2019.	
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/enUS/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/enUS/vulnerability/CVE-2021-34478
8	CVE-2021-34524	- Lỗ hổng tồn tại trong Microsoft Dynamics 365 (onpremises), 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 và 9.1	https://msrc.microsoft.com/update-guide/enUS/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/enUS/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/enUS/vulnerability/CVE-2021-34484