UBND TỈNH THANH HÓA
SỞ THÔNG TIN VÀ TRUYỀN THÔNG

Số: 2808/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 HOÀ XÃ HỘI CHỦ NGHĨA VIỆT NAM
Độc lập - Tự do - Hạnh phúc

Thanh Hoá, ngày 27 tháng 12 năm 2021

Kính gửi:
- VP Tỉnh ủy, VP HĐND tỉnh, VP UBND tỉnh;
- Các sở, ban, ngành cấp tỉnh;
- UBND các huyện, thị xã, thành phố;
- Các tổ chức đoàn thể chính trị cấp tỉnh;
- Các doanh nghiệp viễn thông, CNTT trên địa bàn tỉnh.

Thực hiện công văn số 1749/CATTT-NCSC ngày 15 tháng 12 năm 2021 của Cục An toàn thông tin, Bộ Thông tin và Truyền thông về việc 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 67 lỗ hổng bảo mật mới trên các sản phẩm của hãng Microsoft công bố trong tháng 12 năm 2021. Trong đó, đáng chú ý là 10 lỗ hổng bảo mật có mức ảnh hưởng cao và nghiêm trọng (*thông tin chi tiết có tại phụ lục kèm theo*). Các lỗ hổng trên cho phép đối tượng tấn công sau khi khai thác thành công có thể thực thi mã từ xa, nâng cao đặc quyền trên hệ thống mục tiêu, từ đó chiếm quyền điều khiển toàn bộ hệ thống.

Để tăng cường chủ động phòng ngừa các rủi ro mất an toàn thông tin tại các hệ thống thông tin của các cơ quan, tổ chức và doanh nghiệp do các hình thức tấn công trên có thể xảy ra, Sở Thông tin và Truyền thông đề nghị các cơ quan, đơn vị chỉ đạo các bộ phận, cá nhân thực hiện những nội dung sau:

1. Kiểm tra, rà soát và xác định các máy tính sử dụng hệ điều hành Windows có khả năng bị ảnh hưởng bởi các lỗ hổng trên để có phương án xử lý, khắc phục lỗ hổng. Thực hiện cập nhật bản vá bảo mật cho các máy tính bị ảnh hưởng theo khuyến nghị của hãng Microsoft và các văn bản hướng dẫn của Sở Thông tin và Truyền thông trong thời gian qua. Hướng dẫn kỹ thuật cách thức thực hiện chi tiết tại địa chỉ: ***https://attt.thanhhoa.gov.vn***

2. 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.

Trong quá trình thực hiện, nếu gặp khó khăn, vướng mắc về kỹ thuật liên quan đến các nội dung, công việc trên đề nghị liên hệ với Trung tâm Công nghệ

thông tin và Truyền thông Thanh Hóa (cơ quan thường trực của Đội ứng cứu sự cố an toàn thông tin mạng của tỉnh) để phối hợp hỗ trợ, xử lý.

Điện thoại: (0237)3718.699

Thư điện tử: ungcuusuco@thanhhoa.gov.vn

Xin trân trọng cảm ơn./.

Nơi nhận:
- Như trên;
- Cục An toàn thông tin (để b/c);
- Giám đốc Sở (để b/c);
- Lưu: VT, TTCNTT&TT.

KT.GIÁM ĐỐC
PHÓ GIÁM ĐỐC

CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM
SỞ THÔNG TIN VÀ TRUYỀN THÔNG
TỈNH THANH HÓA

Nguyễn Văn Tước

Phụ lục: Thông tin các lỗ hổng bảo mật
(Kèm theo công văn số /STTTT-CNTT ngày tháng năm 2021 của Sở Thông tin và Truyền thông)

1. Thông tin các 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/en-US/vulnerability/CVE-2021-43890
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/update-guide/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/update-guide/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/en-US/vulnerability/CVE-2021-43899
5	CVE-2021-43215	- Điểm CVSS: 9.8 (Nghiêm trọng)	https://msrc.microsoft.com/update-

		- 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.	guide/vulnerability/CVE-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/update-guide/vulnerability/CVE-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/update-guide/vulnerability/CVE-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/update-guide/vulnerability/CVE-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 10/11, Windows Server 2022.	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-43240

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/update-guide/vulnerability/CVE-2021-43883

2. Hướng dẫn khắc phục

Hướng dẫn chi tiết khắc phục các lỗ hổng bảo mật trên tại địa chỉ: **https://attt.thanhhoa.gov.vn** (*Mục Hướng dẫn → Kỹ năng An toàn thông tin*)