SỞ THÔNG TIN VÀ TRUYỀN THÔNG
THANH HÓA
TRUNG TÂM CNTT&TT

Số: 41 /TTCNTT&TT-QTHT
V/v cảnh báo các lỗ hổng bảo mật mới mức độ cao và nghiêm trọng trong các sản phẩm Microsoft công bố tháng 4/2022

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

Thanh Hoá, ngày 18 tháng4 năm 2022

Kính gửi:
- Văn Phòng Tỉnh ủy;
- Văn Phòng Đoàn ĐBQH và HĐND tỉnh;
- Văn Phòng 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.

Căn cứ Công văn số 508/CATTT-NCSC ngày 13/4/2022 của Cục An toàn thông tin, Bộ Thông tin và Truyền thông về lỗ hổng bảo mật ảnh hưởng cao và nghiêm trọng trong các sản phẩm Microsoft công bố tháng 4/2022. Theo đó, ngày 12/4/2022, hãng Microsoft đã phát hành danh sách bản vá tháng 4 với 128 lỗ hổng bảo mật trong các sản phẩm của mình. Trong đó, bao gồm các lỗ hổng bảo mật có mức ảnh hưởng nghiêm trọng (***CVE-2022-26809, CVE-2022-24491, CVE-2022-24497***) và cao (***CVE-2022-26815, CVE-2022-26904, CVE-2022-26919, CVE-2022-24521***). Theo đánh giá, nếu khai thác thành công các lỗ hổng này cho phép đối tượng tấn công nâng cao đặc quyền từ xa trên hệ thống mục tiêu, từ đó có thể khai thác chiếm quyền điều khiển toàn bộ hệ thống. Trong đó, một số lỗ hổng đã có mã khai thác được đăng tải công khai trên Internet (*Chi tiết các lỗ hổng tại Phụ lục kèm theo*).

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, địa phương do hình thức tấn công trên có thể xảy ra, Trung tâm Công nghệ 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, máy chủ đang cài đặt các phần mềm, ứng dụng có khả năng bị ảnh hưởng bởi các lỗ hổng trên 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. Đối với các thiết bị đang sử dụng các phiên bản của hệ điều hành Windows chưa có bản vá bảo mật, chưa được cài đặt phần mềm phòng chống mã độc tập trung của tỉnh cần thực hiện biện pháp khắc phục thay thế để giảm thiểu nguy cơ tấn công. Hướng dẫn kỹ

thuật cách thức thực hiện chi tiết đối với từng lỗ hổng bảo mật tại địa chỉ: https://attt.thanhhoa.gov.vn

2. Tăng cường giám sát và sẵn sàng phương án xử lý khi phát hiện có dấu hiệu bị khai thác, tấn công mạng; đồng thời thường xuyên theo dõi kênh cảnh báo của các cơ quan chức năng và các tổ chức lớn về an toàn thông tin để phát hiện kịp thời các nguy cơ 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 kính gửi;
- Sở TT&TT (để b/c);
- PGĐ Sở Nguyễn Văn Tước (để b/c);
- Giám đốc Trung tâm (để b/c);
- Lưu: VT, QTHT.

KT. GIÁM ĐỐC
PHÓ GIÁM ĐỐC

SỞ THÔNG TIN VÀ TRUYỀN THÔNG TỈNH THANH HÓA
TRUNG TÂM CÔNG NGHỆ THÔNG TIN VÀ TRUYỀN THÔNG

Trần Ngọc Hưng

Phụ lục: Thông tin các lỗ hổng bảo mật
(Kèm theo công văn số /TTCNTT-QTHT ngày tháng năm 2022 của Trung tâm Công nghệ thông tin và Truyền thông Thanh Hóa)

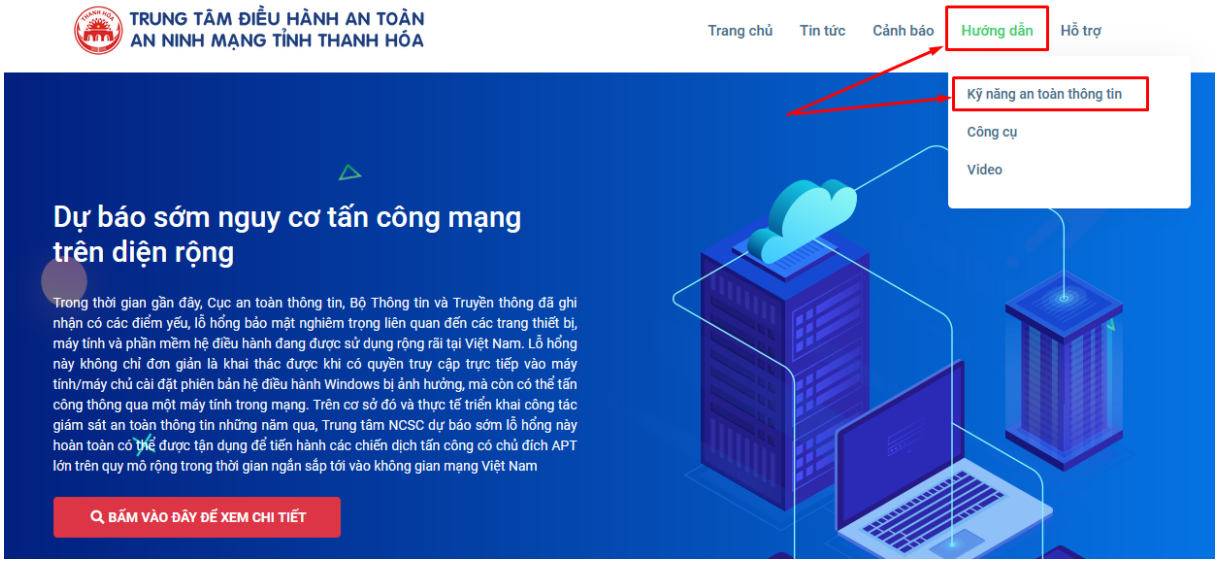
1. Thông tin lỗ hổng bảo mật

STT	CVE	Mô tả	Link tham khảo
1	CVE-2022-26809	- Điểm CVSS: 9.8 (Nghiêm trọng) - Lỗ hổng trong RPC Runtime Library cho phép đối tượng tấn công thực thi mã từ xa với đặc quyền cao trên hệ thống bị ảnh hưởng. - Ảnh hưởng: Windows 7/8.1/10/11, Windows Server 2008/2012/2016/2019/2022.	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-26809
2	CVE-2022-24491	- Điểm CVSS: 9.8 (Nghiêm trọng) - Lỗ hổng trong Windows Network File System cho phép đối tượng tấn công thực thi mã từ xa với đặc quyền cao. - Ảnh hưởng: Windows 8.1/10/11, Windows Server 2012/2016/2019.	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-24491
3	CVE-2022-24497	- Điểm CVSS: 9.8 (Nghiêm trọng) - Lỗ hổng trong Windows Network File System cho phép đối tượng tấn công thực thi mã từ xa. - Ảnh hưởng: Windows 8.1/10, Windows Server 2012/2016/2019/2022.	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-24497
4	CVE-2022-26815	- Điểm CVSS: 7.2 (cao) - Lỗ hổng trong Windows DNS Server cho phép đối tượng tấn công thực thi mã từ xa.	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-26815

		- Ảnh hưởng: Windows Server 2008/2012/2016/2019/2022.	
5	CVE-2022-26904	- Điểm CVSS: 7.9 (cao) - Lỗ hổng trong Windows User Profile Service cho phép đối tượng tấn công thực hiện nâng cao đặc quyền. Lỗ hổng này đã có mã khai thác công khai trên Internet. - Ảnh hưởng: Windows 7/8.1/10/11, Windows Server 2008/2012/2016.	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-26904
6	CVE-2022-26919	- Điểm CVSS: 8.1 (Cao) - Lỗ hổng trong Windows LDAP cho phép đối tượng tấn công thực thi mã từ xa. - Ảnh hưởng: Windows 8.1/10/11, Windows Server 2008/2012/2016/2019/2022.	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-26919
7	CVE-2022-24521	- Điểm CVSS: 7.8 (Cao) - Lỗ hổng trong Windows Common Log File System Driver cho phép đối tượng tấn công thực hiện nâng cao đặc quyền. - Ảnh hưởng: Windows 7/8.1/10/11, Windows Server 2008/2012/2016/2019/2022.	https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2022-24521

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*)


TRUNG TÂM ĐIỀU HÀNH AN TOÀN
AN NINH MẠNG TỈNH THANH HÓA
Trang chủ
Tin tức
Cảnh báo
Hướng dẫn
Hỗ trợ
Kỹ năng an toàn thông tin
Công cụ
Video
Dự báo sớm nguy cơ tấn công mạng trên diện rộng
Trong thời gian gần đây, Cục an toàn thông tin, Bộ Thông tin và Truyền thông đã ghi nhận có các điểm yếu, lỗ hổng bảo mật nghiêm trọng liên quan đến các trang thiết bị, máy tính và phần mềm hệ điều hành đang được sử dụng rộng rãi tại Việt Nam. Lỗ hổng này không chỉ đơn giản là khai thác được khi có quyền truy cập trực tiếp vào máy tính/máy chủ cài đặt phiên bản hệ điều hành Windows bị ảnh hưởng, mà còn có thể tấn công thông qua một máy tính trong mạng. Trên cơ sở đó và thực tế triển khai công tác giám sát an toàn thông tin những năm qua, Trung tâm NCSC dự báo sớm lỗ hổng này hoàn toàn có thể được tận dụng để tiến hành các chiến dịch tấn công có chủ đích APT lớn trên quy mô rộng trong thời gian ngắn sắp tới vào không gian mạng Việt Nam
BẤM VÀO ĐÂY ĐỂ XEM CHI TIẾT