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

Số: 70 /TTCNTT&TT-QTHT
V/v cảnh báo kết nối mã độc và lỗ hổng an toàn thông tin trong các sản phẩm Microsoft công bố tháng 01/2024.

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

Thanh Hoá, ngày 24 tháng 01 năm 2024

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 VT, CNTT trên địa bàn tỉnh.

Căn cứ Công văn số 66/CATTT-NCSC ngày 17/01/2024 về việc lỗ hổng an toàn thông tin ảnh hưởng cao và nghiêm trọng trong các sản phẩm Microsoft công bố tháng 01/2024 của Cục An toàn thông tin, Bộ Thông tin và Truyền thông. Theo đó, hãng Microsoft đã phát hành danh sách bản vá tháng 01 với 49 lỗ hổng an toàn thông tin trong các sản phẩm của mình. Bản phát hành tháng này đặc biệt đáng chú ý vào các lỗ hổng an toàn thông tin có mức ảnh hưởng cao và nghiêm trọng sau:

- Lỗ hổng an toàn thông tin **CVE-2024-20674** trong Windows Kerberos cho phép đối tượng tấn công vượt qua cơ chế bảo vệ để thực hiện tấn công giả mạo.

- Lỗ hổng an toàn thông tin **CVE-2024-21318** trong Microsoft SharePoint Server cho phép đối tượng tấn công thực thi mã từ xa.

- Lỗ hổng an toàn thông tin **CVE-2024-20677** trong Microsoft Office cho phép đối tượng tấn công thực thi mã từ xa.

- Lỗ hổng an toàn thông tin **CVE-2024-20700** trong Windows Hyper-V cho phép đối tượng tấn công thực thi mã từ xa.

(Thông tin chi tiết các lỗ hổng bảo mật có tại Phụ lục 01 kèm theo.)

Hiện nay, qua theo dõi trên hệ thống Trung tâm Điều hành an toàn, an ninh mạng của tỉnh, đang ghi nhận tại hệ thống mạng của các cơ quan, đơn vị có lây nhiễm mã độc, kết nối đến các hệ thống do tin tặc điều khiển. Đồng thời chưa thực hiện cập nhật các lỗ hổng bảo mật đã cảnh báo trước đây trên các máy tính của cán bộ công chức, viên chức (*danh sách các đơn vị theo Phụ lục 02 kèm theo*).

Để bảo đảm an toàn thông tin mạng đối với các hệ thống thông tin trong các cơ quan nhà nước trên địa bàn tỉnh, Trung tâm Công nghệ thông tin và Truyền thông Thanh Hóa đề nghị các cơ quan, đơn vị chỉ đạo các bộ phận, cá nhân thực hiện những nội dung sau:

1. Rà soát và xác định máy tính trong phạm vi cơ quan, các đơn vị trực thuộc và UBND cấp xã đang sử dụng hệ điều hành Windows có khả năng bị ảnh hưởng (nếu có), thực hiện cập nhật bản vá kịp thời để tránh nguy cơ bị tấn công (*Hướng dẫn chi tiết tại địa chỉ: https://attt.thanhhoa.gov.vn*).

2. Các cơ quan, đơn vị đang có kết nối mã độc tiến hành kiểm tra, rà soát và khoanh vùng tìm kiếm để gỡ bỏ mã độc đang lây nhiễm trên các máy tính trong hệ thống mạng của đơn vị.

3. Chỉ đạo Tổ ứng cứu sự cố an toàn thông tin mạng tại cơ quan, địa phương mình triển khai rà soát và sẵn sàng phương án xử lý sự cố 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.

Sau khi thực hiện, đề nghị các cơ quan, đơn vị báo cáo số liệu (số máy đã xử lý/tổng số máy) về 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*) trước ngày 30/01/2024 để tổng hợp.

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 để phối hợp hỗ trợ, xử lý.

Điện thoại: (0237)3718.699; Thư điện tử: ungcuusuco@thanhhoa.gov.vn./.

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 01: Thông tin các lỗ hổng bảo mật tháng 01/2024
(Kèm theo công văn số /TTCNTT&TT-QTHT ngày tháng năm 2024 của Trung tâm Công nghệ thông tin và Truyền thông Thanh Hóa)

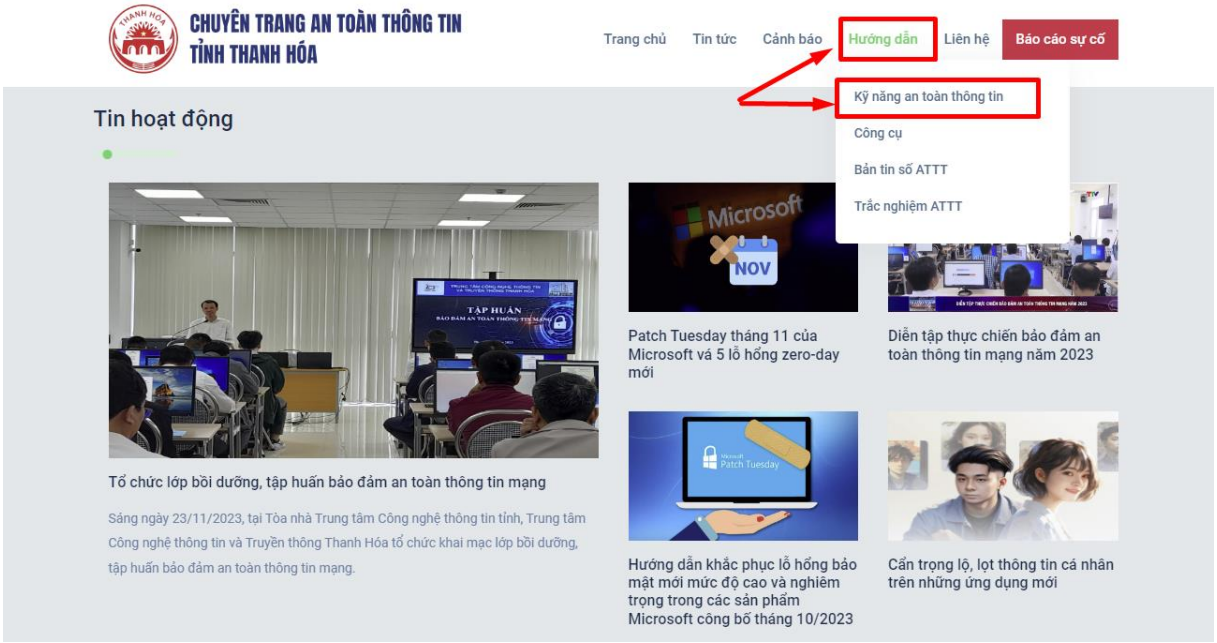
1. Thông tin các lỗ hổng bảo mật

STT	CVE	Mô tả	Địa chỉ tham khảo
1	CVE-2024-20674	- Điểm: CVSS: 9.0 (Nghiêm trọng) - Mô tả: Lỗ hổng trong Windows Kerberos cho phép đối tượng tấn công vượt qua cơ chế bảo vệ để thực hiện tấn công giả mạo. - Ảnh hưởng: Windows 10, Windows 11; Windows Server 2008, 2012, 2016, 2019, 2022.	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-20674
2	CVE-2024-21318	- Điểm: CVSS: 8.8 (Cao) - Mô tả: Lỗ hổng trong Microsoft SharePoint Server cho phép đối tượng tấn công thực thi mã từ xa. - Ảnh hưởng: Microsoft SharePoint Server 2016, 2019; Microsoft SharePoint Server Subscription Edition.	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-21318
3	CVE-2024-20677	- Điểm: CVSS: 7.8 (Cao) - Mô tả: Lỗ hổng trong Microsoft Office cho phép đối tượng tấn công thực thi mã từ xa. - Ảnh hưởng: Microsoft Office 2019; Microsoft Office LTSC; Microsoft 365 Apps.	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-20677

STT	CVE	Mô tả	Địa chỉ tham khảo
4	CVE-2024-20700	- Điểm: CVSS: 7.5 (Nghiêm trọng) - Mô tả: Lỗ hổng trong Windows Hyper-V cho phép đối tượng tấn công thực thi mã từ xa. - Ảnh hưởng: Windows 10, Windows 11; Windows Server 2019, 2022.	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-20700

2. Hướng dẫn khắc phục

Biện pháp tốt nhất để khắc phục là cập nhật bản vá cho các lỗ hổng an toàn thông tin nói trên theo hướng dẫn của hãng. 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*). 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. Tài liệu tham khảo

- https://msrc.microsoft.com/update-guide/
- https://www.zerodayinitiative.com/blog/2024/1/9/the-january-2024-security-update-review

Phụ lục 02: Thông tin các đơn vị có kết nối mã độc

(Kèm theo công văn số /TTCNTT&TT-QTHT ngày tháng năm 2024 của Trung tâm Công nghệ thông tin và Truyền thông Thanh Hóa)

STT	Tên đơn vị	Địa chỉ kết nối mã độc
1	Sở Nông nghiệp phát triển Nông thôn	34.91.94.238
2	Sở Tài Nguyên & Môi trường	34.91.32.224
3	UBND huyện Bá Thước	184.105.192.2
4	UBND huyện Ngọc Lặc	34.150.171.112
5	UBND huyện Yên Định	35.247.124.134
		34.101.226.87
		34.150.171.112
		34.91.94.238