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

Số: 94 /TTCNTT&TT-QTHT
V/v lỗ hổng an toàn thông tin ảnh hưởng cao và nghiêm trọng trong các sản phẩm Microsoft công bố tháng 02/2024.

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

Thanh Hoá, ngày 27 tháng 02 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 210/CATTT-NCSC ngày 22/02/2024 về việc lỗ hổng an toàn thông tin ảnh hưởng cao và nghiêm trọng trong các sản phẩm Microsoft công bố tháng 02/2024 của Cục An toàn thông tin, Bộ Thông tin và Truyền thông. Theo đó, ngày 13/02/2024, Microsoft đã phát hành danh sách bản vá tháng 02 với 72 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-2024-21410** trong Microsoft Exchange Server cho phép đối tượng không cần xác thực thực hiện tấn công leo thang đặc quyền. Lỗ hổng hiện đang bị khai thác trong thực tế.

- 02 lỗ hổng an toàn thông tin **CVE-2024-21413, CVE-2024-21378** trong Microsoft Outlook cho phép đối tượng tấn công không cần xác thực thực thi mã từ xa.

- Lỗ hổng an toàn thông tin **CVE-2024-21399** trong Microsoft Edge (Chromium-based) cho phép đối tượng tấn công thực thi mã từ xa.

- Lỗ hổng an toàn thông tin **CVE-2024-21412** trong Internet Shortcut Files cho phép đối tượng tấn công vượt qua cơ chế bảo mật. Lỗ hổng hiện đang bị khai thác trong thực tế.

- Lỗ hổng an toàn thông tin **CVE-2024-21379** trong Microsoft Word cho phép đối tượng tấn công thực thi mã từ xa.

- Lỗ hổng an toàn thông tin **CVE-2024-21384** trong Microsoft Office OneNote cho phép đối tượng tấn công thực thi mã từ xa.

- Lỗ hổng an toàn thông tin **CVE-2024-20673** trong Microsoft Office cho phép đối tượng tấn công thực thi mã từ xa.

- Lỗ hổng an toàn thông tin **CVE-2024-21351** trong Windows SmartScreen cho phép đối tượng tấn công vượt qua cơ chế bảo mật. Lỗ hổng hiện đang bị khai thác trong thực tế.

(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, 03 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. Tổ chức kiểm tra, 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 và chưa cập nhật đầy đủ các lỗ hổng bảo mật trên các máy tính đã khuyến nghị. Đề nghị khẩn trương 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 chủ động 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 phổ biến, tuyên truyền kịp thời các nguy cơ về mất an toàn thông tin được cảnh báo của các cơ quan chức năng trong phạm vi cơ quan, địa phương.

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 11/03/2024 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

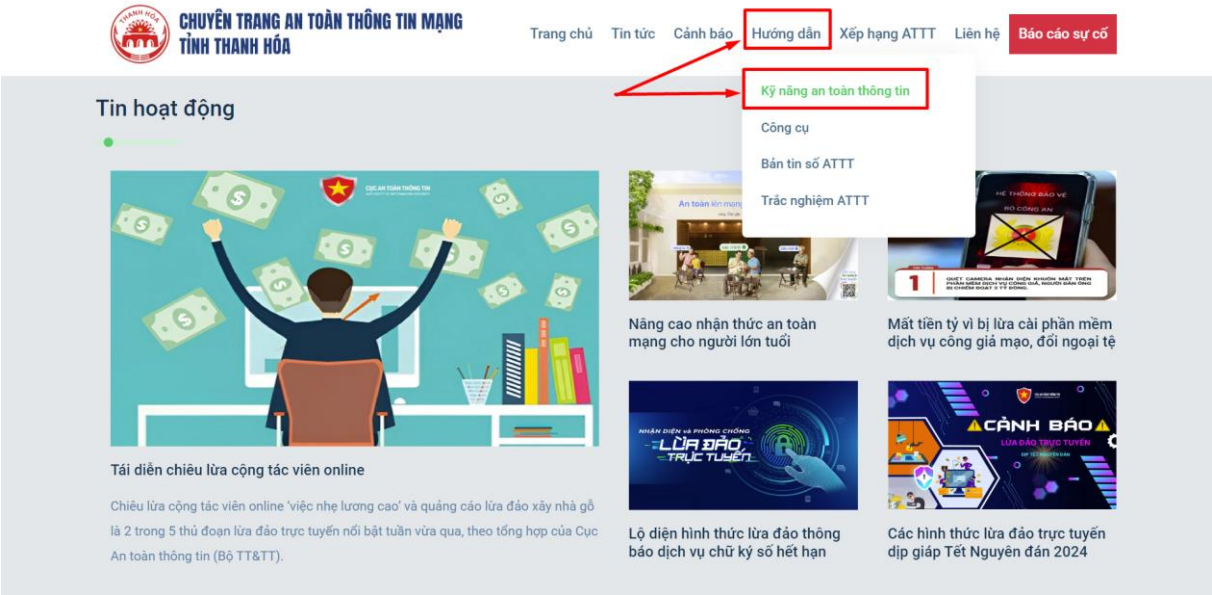
STT	CVE	Mô tả	Link tham khảo
1	CVE-2024-21410	- Điểm: CVSS: 9.8 (Nghiêm trọng) - Mô tả: Lỗ hổng trong Microsoft Exchange Server cho phép đối tượng không cần xác thực thực hiện tấn công leo thang đặc quyền. Lỗ hổng hiện đang bị khai thác trong thực tế. - Ảnh hưởng: Microsoft Exchange Server 2016, 2019.	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-21410
2	CVE-2024-21413 CVE-2024-21378	- Điểm: CVSS: 9.8 (Nghiêm trọng) - Mô tả: Lỗ hổng trong Microsoft Outlook cho phép đối tượng tấn công không cần xác thực thực thi mã từ xa. - Ảnh hưởng: Microsoft Office, Microsoft Office LTSC, Microsoft 365 Apps for Enterprise, Microsoft Outlook.	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-21413 https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-21378
3	CVE-2024-21399	- Điểm: CVSS: 8.3 (Trung bình) - Mô tả: Lỗ hổng trong Microsoft Edge (Chromium-based) cho phép đối tượng tấn công thực thi mã từ xa. - Ảnh hưởng: Microsoft Edge (Chromium-based).	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-21399

4	CVE-2024-21412	- Điểm: CVSS: 8.1 (Cao) - Mô tả: Lỗ hổng trong Internet Shortcut Files cho phép đối tượng tấn công vượt qua cơ chế bảo mật. Lỗ hổng hiện đang bị khai thác trong thực tế. - Ảnh hưởng: Windows 10, Windows 11, Windows Server 2019, 2022.	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-21412
5	CVE-2024-21379	- Điểm: CVSS: 7.8 (Cao) - Mô tả: Lỗ hổng trong Microsoft Word cho phép đối tượng tấn công thực thi mã từ xa. - Ảnh hưởng: Microsoft Word, Microsoft Office, Microsoft Office LTSC, Microsoft 365 Apps for Enterprise.	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-21379
6	CVE-2024-21384	- Điểm: CVSS: 7.8 (Cao) - Mô tả: Lỗ hổng trong Microsoft Office OneNote cho phép đối tượng tấn công thực thi mã từ xa. - Ảnh hưởng: Microsoft Office LTSC, Microsoft 365 Apps for Enterprise.	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-21384
7	CVE-2024-20673	- 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 LTSC, Microsoft Office, Skype for Business.	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-20673

8	CVE-2024-21351	- Điểm: CVSS: 7.6 (Cao) - Mô tả: Lỗ hổng trong Windows SmartScreen cho phép đối tượng tấn công vượt qua cơ chế bảo mật. Lỗ hổng hiện đang bị khai thác trong thực tế. - Ảnh hưởng: Windows 10, Windows 11, Windows Server 2016, 2019, 2022.	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-21351

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/2024/2/13/the-february-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	Đơn vị bị nhiễm	IP	Địa chỉ kết nối mã độc
1	Sở Nông nghiệp phát triển Nông thôn	113.160.181.5	34.91.94.238
			35.247.124.134
			34.101.226.87
2	Sở Tài nguyên và Môi trường	113.160.187.187	34.91.32.224
3	UBND huyện Bá Thước	113.160.182.204	184.105.192.2
4	UBND huyện Ngọc Lặc	113.160.185.0	184.105.192.2
5	UBND huyện Nông Cống	14.241.85.233	34.101.226.87
			34.91.94.238
			35.247.124.134
6	UBND huyện Yên Định	113.160.183.96	34.91.94.238
			34.101.226.87
			35.247.124.134
			34.150.171.112
7	UBND huyện Quảng Xương	113.160.182.236	34.101.226.87

Phụ lục 03: Thống kê các máy tính chưa cập nhật lỗ hổng bảo mật

(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	Đơn vị	Số lượng máy chưa cập nhật lỗ hổng bảo mật
I	**Các Cơ quan, đơn vị cấp Sở**	
1	Ban Quản lý Khu kinh tế Nghi Sơn	49
2	Sở Kế hoạch và Đầu tư	45
3	Sở Nông nghiệp và Phát triển nông thôn	33
4	Sở Xây dựng	31
5	Sở Lao động, Thương binh và Xã hội	30
6	Sở Giao thông vận tải	27
7	Sở Tài nguyên và Môi trường	25
9	Sở Tư pháp	25
10	Sở Văn hóa, thể thao và Du lịch	25
11	Sở Công thương	12
12	Ban Dân tộc	8
13	Sở Y tế	8
14	Sở Ngoại vụ	6
16	Sở Giáo dục và Đào tạo	5
17	Sở Nội vụ	5
18	Sở Khoa học và Công nghệ	3
19	Thanh tra tỉnh	3
II	**UBND cấp huyện**	
1	UBND huyện Đông Sơn	55
2	UBND TX Nghi Sơn	43
3	UBND huyện Thọ Xuân	35
4	UBND huyện Hà Trung	29
5	UBND huyện Thạch Thành	29
6	UBND thành phố Thanh Hóa	27
7	UBND huyện Cẩm Thủy	25
8	UBND huyện Hoằng Hóa	21
9	UBND huyện Yên Định	21
10	UBND huyện Thiệu Hóa	20
11	UBND huyện Triệu Sơn	20
12	UBND huyện Vĩnh Lộc	20

13	UBND huyện Bá Thước	14
14	UBND huyện Quảng Xương	12
15	UBND huyện Nga Sơn	11
16	UBND huyện Quan Hóa	11
17	UBND huyện Thường Xuân	10
18	UBND huyện Như Thanh	9
19	UBND huyện Nông Cống	9
20	UBND thị xã Bỉm Sơn	9
21	UBND huyện Mường Lát	8
22	UBND huyện Quan Sơn	8
23	UBND huyện Như Xuân	7
24	UBND thành phố Sầm Sơn	7
25	UBND huyện Ngọc Lặc	6
26	UBND huyện Lang Chánh	3
27	UBND huyện Hậu Lộc	2