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

Số: 192 /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 08/2023.

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

Thanh Hoá, ngày 29 tháng 8 năm 2023

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 1500/CATTT-NCSC ngày 21/8/2023 về việc lỗ hổng an toàn thông tin ảnh hưởng cao và nghiêm trọng trong các sản phẩm Microsoft công bố tháng 08/2023 của Cục An toàn thông tin Bộ Thông tin và Truyền thông. Theo đó ngày 08/8/2023, Microsoft đã phát hành danh sách bản vá tháng 8 với 74 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-2023-38181 trong Microsoft Exchange Server cho phép đối tượng tấn công thực hiện tấn công Spoofing. Đối tượng tấn công có thể khai thác lỗ hổng này để vượt qua bản vá cho một lỗ hổng đã bị khai thác trong thực tế, CVE-2022-41082.

- Lỗ hổng an toàn thông tin CVE-2023-21709 trong Microsoft Exchange Server cho phép đối tượng tấn công thực hiện tấn công nâng cao đặc quyền.

- 04 lỗ hổng an toàn thông tin CVE-2023-35368, CVE-2023-38185, CVE-2023-35388, CVE-2023-38182 trong Microsoft Exchange Server cho phép đối tượng tấn công thực thi mã từ xa.

- 03 lỗ hổng an toàn thông tin CVE-2023-35385, CVE-2023-36910, CVE-2023-36911 trong Microsoft Message Queuing cho phép đối tượng tấn công thực thi mã từ xa.

- 02 lỗ hổng an toàn thông tin CVE-2023-29328, CVE-2023-29330 trong Microsoft Teams cho phép đối tượng tấn công thực thi mã từ xa.

- Lỗ hổng an toàn thông tin CVE-2023-36895 trong Microsoft Outlook cho phép đối tượng tấn công thực thi mã từ xa.

- Lỗ hổng an toàn thông tin CVE-2023-36896 trong Microsoft Excel cho phép đối tượng tấn công thực thi mã từ xa.

- Lỗ hổng an toàn thông tin CVE-2023-35371 trong Microsoft Office cho phép đối tượng tấn công thực thi mã từ xa.

(Thông tin chi tiết các lỗ hổng bảo mật có 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, đơn vị, 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. Kiểm tra, rà soát, xác định máy sử dụng hệ điều hành Windows có khả năng bị ảnh hưởng bởi các lỗ hổng bảo mật được công bố trên. Thực hiện cập nhật bản vá bảo mật đối với các lỗ hổng này kịp thời để tránh nguy cơ bị tấn công. Hướng dẫn kỹ thuật cách thức thực hiện chi tiết đối với lỗ hổng bảo mật tại địa chỉ: https://attt.thanhhoa.gov.vn

2. Chỉ đạo các Tổ ứng cứu sự cố an toàn thông tin mạng tại cơ quan, đơn vị mình tăng cường giám sát hoạt động các hệ thống thông tin 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.

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&TT-QTHT ngày tháng năm 2023 của Trung tâm Công nghệ thông tin và Truyền thông Thanh Hóa)

1. Thông tin các lỗ hổng bảo mật

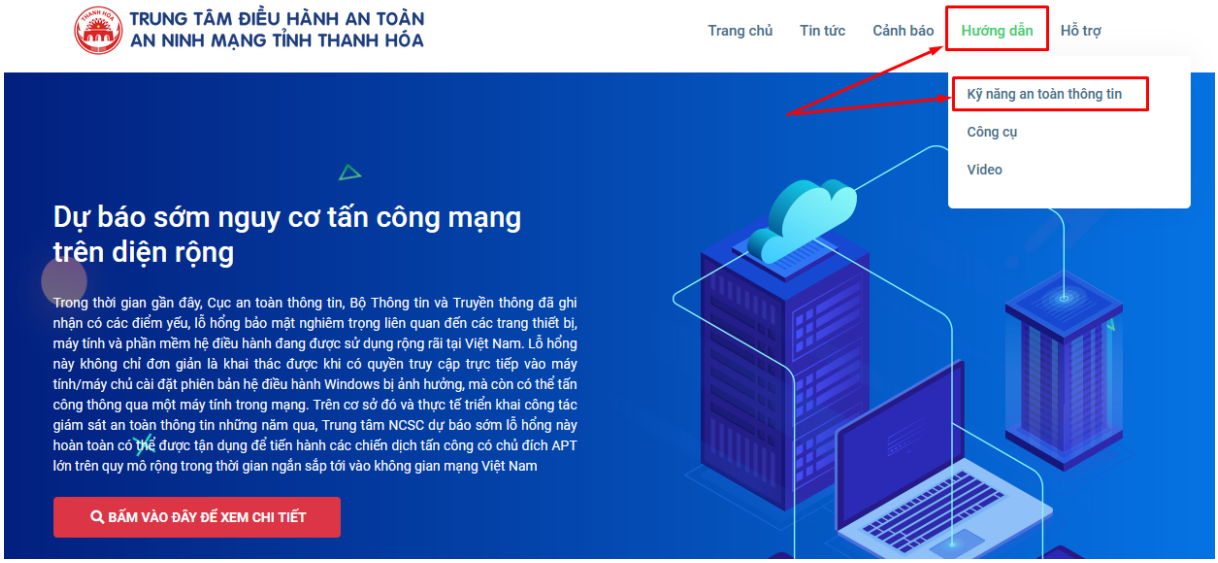
STT	CVE	Mô tả	Link tham khảo
1	CVE-2023-38181	- Điểm: CVSS: 8.8 (Cao) - Mô tả: lỗ hổng trong Microsoft Exchange Server cho phép đối tượng tấn công thực hiện tấn công Spoofing. - Ảnh hưởng: Exchange Server 2016/2019.	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-38181
2	CVE-2023-21709	- Điểm: CVSS: 9.8 (được Microsoft đánh giá là Cao) - Mô tả: lỗ hổng trong Microsoft Exchange Server cho phép đối tượng tấn công thực hiện tấn công nâng cao đặc quyền. - Ảnh hưởng: Exchange Server 2016/2019.	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-21709
3	CVE-2023-35368 CVE-2023-38185 CVE-2023-35388 CVE-2023-38182	- Điểm: CVSS: 8.0/8.8 (Cao) - Mô tả: lỗ hổng trong Microsoft Exchange Server cho phép đối tượng tấn công thực thi mã từ xa. - Ảnh hưởng: Exchange Server 2016/2019.	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-35368 https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-38185 https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-35388 https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-38182

STT	CVE	Mô tả	Link tham khảo
4	CVE-2023-35385 CVE-2023-36910 CVE-2023-36911	- Điểm: CVSS: 9.8 (Nghiêm trọng) - Mô tả: lỗ hổng trong Microsoft Message Queuing cho phép đối tượng tấn công thực thi mã từ xa. - Ảnh hưởng: Windows 10/11, Windows Server.	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-35385 https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-36910 https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-36911
5	CVE-2023-29328 CVE-2023-29330	- Điểm: CVSS: 8.8 (được Microsoft đánh giá là Nghiêm trọng) - Mô tả: lỗ hổng trong Microsoft Teams cho phép đối tượng tấn công thực thi mã từ xa. - Ảnh hưởng: Microsoft Teams dành cho iOS, Mac, Android, Desktop	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-29328 https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-29330
6	CVE-2023-36895	- Điểm: CVSS: 7.8 (được Microsoft đánh giá là Nghiêm trọng) - Mô tả: lỗ hổng trong Microsoft Outlook cho phép đối tượng tấn công thực thi mã từ xa. - Ảnh hưởng: Microsoft Office, Microsoft 365 Apps for Enterprise.	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-36895
7	CVE-2023-36896	- Điểm: CVSS: 7.8 (Cao) - Mô tả: lỗ hổng trong Microsoft Excel cho phép đối tượng tấn công thực thi mã từ xa.	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-36896

STT	CVE	Mô tả	Link tham khảo
		- Ảnh hưởng: Microsoft Excel, Office, Office LTSC, 365 Apps.	
8	CVE-2023-35371	- 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, Office LTSC, 365 Apps.	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-35371

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*)



3. Tài liệu tham khảo

https://msrc.microsoft.com/update-guide

https://www.zerodayinitiative.com/blog/2023/8/8/the-august-2023-security-update-review