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

Số: 156 /TTCNTT&TT-QTHT
V/v lỗ hổng an toàn thông tin ảnh hưởng cao và nghiêm trọng trong các sản phẩm của Microsoft công bố tháng 07/2023.

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

Thanh Hoá, ngày tháng 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 1261/CATTT-NCSC ngày 17/7/2023 của Cục An toàn thông tin, Bộ Thông tin và Truyền thông về việc cảnh lỗ hổng bảo mật ảnh hưởng cao và nghiêm trọng trong các sản phẩm Microsoft công bố tháng 07/2023.

Theo đó, ngày 11/07/2023, hãng Microsoft đã phát hành danh sách bản vá bảo mật trong tháng 07/2023 với 130 lỗ hổng an toàn thông tin trong các sản phẩm của mình. Bản phát hành tháng này đặc biệt đáng chú ý các lỗ hổng an toàn thông tin có mức ảnh hưởng cao và nghiêm trọng như sau:

- 02 lỗ hổng an toàn thông tin **CVE-2023-33160, CVE-2023-33134** trong sản phẩm Microsoft SharePoint Server cho phép đối tượng tấn công thực thi mã khai thác từ xa.

- Lỗ hổng an toàn thông tin **CVE-2023-36884** trong sản phẩm Office và Windows cho phép đối tượng tấn công thực thi mã khai thác từ xa khi người dùng mở tệp tài liệu của Microsoft Office do đối tượng tấn công tạo ra. Lỗ hổng này hiện đang bị khai thác trong thực tế.

- Lỗ hổng an toàn thông tin **CVE-2023-35311** trong sản phẩm Microsoft Outlook cho phép đối tượng tấn công thực hiện tấn công vượt qua cơ chế bảo mật (Bypass). Lỗ hổng này hiện đang bị khai thác trong thực tế.

- Lỗ hổng an toàn thông tin **CVE-2023-36874** trong dịch vụ Windows Error Reporting Service cho phép đối tượng tấn công thực hiện tấn công nâng cao đặc quyền. Lỗ hổng này hiện đang bị khai thác trong thực tế.

- Lỗ hổng an toàn thông tin **CVE-2023-32046** trong Windows MSHTML cho

phép đối tượng tấn công thực hiện tấn công nâng cao đặc quyền. Lỗ hổng này hiện đang bị khai thác trong thực tế.

- Lỗ hổng an toàn thông tin **CVE-2023-32049** trong Windows SmartScreen cho phép đối tượng tấn công thực hiện tấn công vượt qua cơ chế bảo mật (Bypass). Lỗ hổng này hiện đang bị khai thác trong thực tế.

- 02 lỗ hổng an toàn thông tin **CVE-2023-32057, CVE-2023-35309** trong Microsoft Message Queuing 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. Khẩn trương thực hiện kiểm tra, rà soát, xác định các máy tính của người dùng trong cơ quan, đơn vị 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 khắc phục chi tiết 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 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: (02373)718.699; 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 tháng 07/2023
(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

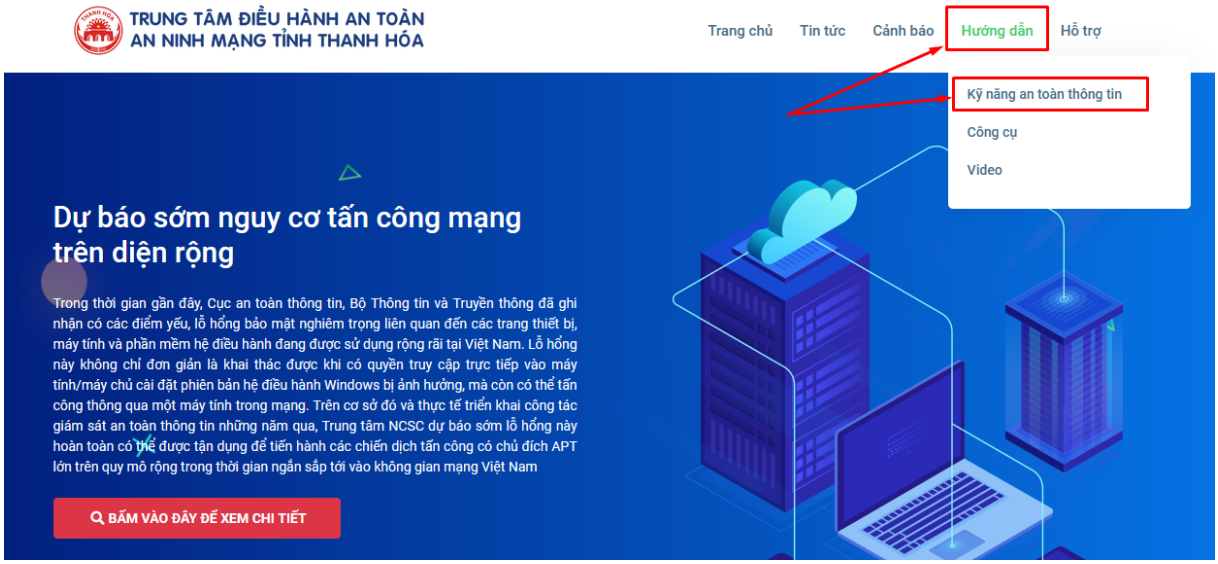
STT	CVE	Mô tả	Link tham khảo
1	CVE-2023-33160 CVE-2023-33134	- Điểm: CVSS: 8.8 (Cao) - Mô tả: lỗ hổng trong Microsoft SharePoint Server cho phép đối tượng tấn công thực thi mã từ xa. - Ảnh hưởng: Microsoft SharePoint Server.	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-33160 https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-33134
2	CVE-2023-36884	- Điểm: CVSS: 8.3 (Cao) - Mô tả: lỗ hổng trong Office và Windows HTML cho phép đối tượng tấn công thực thi mã từ xa. - Ảnh hưởng: Windows 10, 11, Windows Server, Microsoft Office.	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-36884
3	CVE-2023-35311	- Điểm: CVSS: 8.8 (Cao) - Mô tả: lỗ hổng trong Microsoft Outlook cho phép đối tượng tấn công thực hiện tấn công vượt qua cơ chế bảo mật (Bypass). - Ảnh hưởng: Microsoft 365, Microsoft Office, Microsoft Outlook.	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-35311
4	CVE-2023-36874	- Điểm: CVSS: 7.8 (Cao) - Mô tả: lỗ hổng trong Windows Error Reporting Service cho phép đối tượng	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-36874

STT	CVE	Mô tả	Link tham khảo
		tấn công thực hiện tấn công nâng cao đặc quyền. - Ảnh hưởng: Windows Server, Windows 10/11.	
5	CVE-2023-32046	- Điểm: CVSS: 7.8 (Cao) - Mô tả: lỗ hổng trong Windows MSHTML cho phép đối tượng tấn công thực hiện tấn công nâng cao đặc quyền. - Ảnh hưởng: Windows Server, Windows 10/11.	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-32046
6	CVE-2023-32049	- Điểm: CVSS: 8.8 (Cao) - Mô tả: lỗ hổng trong Windows SmartScreen cho phép đối tượng tấn công thực hiện tấn công vượt qua cơ chế bảo mật (Bypass). - Ảnh hưởng: Windows Server, Windows 10/11.	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-32049
7	CVE-2023-32057 CVE-2023-35309	- 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 Server, Windows 10/11.	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-32057 https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-35309

2. Hướng dẫn khắc phục

Biện pháp tốt nhất để khắc phục là cập nhật bản vá bảo mật định kỳ 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/2023/7/10/the-july-2023-security-update-review