UBND TỈNH THỪA THIÊN HUẾ
SỞ THÔNG TIN VÀ TRUYỀN THÔNG

CỘNG HOÀ XÃ HỘI CHỦ NGHĨA VIỆT NAM
Độc lập – Tự do – Hạnh Phúc

Số: 2807/STTTT-IOC
V/v cảnh báo lỗ hổng bảo mật ảnh hưởng Cao và Nghiêm trọng trong các sản phẩm Microsoft công bố tháng 9/2024

Thừa Thiên Huế, ngày 26 tháng 9 năm 2024

Kính gửi:
- Văn phòng Tỉnh ủy;
- Các cơ quan chuyên môn thuộc UBND tỉnh;
- Các đơn vị sự nghiệp thuộc tỉnh;
- UBND các huyện, thị xã và thành phố Huế;
- Các cơ quan, đơn vị, tổ chức khác có kết kết mạng WAN;
- Đại học Huế.

Ngày **10/09/2024**, Microsoft đã phát hành danh sách bản vá tháng **09** với **79 lỗ hổng** an toàn thông tin trong các sản phẩm của mình. Trong đó có **07** lỗ hổng mức Nghiêm trọng và **71** lỗ hổng mức độ Cao. Ngoài ra, Microsoft cũng đã khắc phục được 04 lỗ hổng zero-day đang bị khai thác trong thực tế.

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-2024-43491** trong Microsoft Windows Update cho phép đối tượng tấn công thực thi mã từ xa. Lỗ hổng hiện đang bị khai thác trong thực tế.

- **04** lỗ hổng an toàn thông tin **CVE-2024-38018, CVE-2024-38227, CVE-2024-38228, CVE-2024-43464** trong Microsoft SharePoint Server cho phép đối tượng tấn công thực thi mã từ xa.

- Lỗ hổng an toàn thông tin **CVE-2024-43461** trong Windows MSHTML Platform cho phép đối tượng tấn công thực hiện tấn công giả mạo (spoofing).

- **02** lỗ hổng an toàn thông tin **CVE-2024-21416, CVE-2024-38045** trong Windows TCP/IP cho phép đối tượng tấn công thực thi mã từ xa.

- Lỗ hổng an toàn thông tin **CVE-2024-38014** trong Windows Installer cho phép đối tượng tấn công thực hiện leo thang đặc quyền. Lỗ hổng hiện đang bị khai thác trong thực tế.

- Lỗ hổng an toàn thông tin **CVE-2024-43463** trong Microsoft Office Visio cho phép đối tượng tấn công thực thi mã từ xa.

- Lỗ hổng an toàn thông tin **CVE-2024-38226** trong Microsoft Publisher cho phép đối tượng tấn công vượt qua cơ chế bảo vệ. Lỗ hổng hiện đang bị khai thác trong thực tế.

- **02** lỗ hổng an toàn thông tin **CVE-2024-38217, CVE-2024-43487** trong Windows Mark of the Web cho phép đối tượng tấn công vượt qua cơ chế bảo vệ. Lỗ hổng hiện đang bị khai thác trong thực tế.

Ngoài các lỗ hổng an toàn thông tin nêu trên, còn tồn tại một số lỗ hổng an toàn thông tin khác có thể ảnh hưởng đến hệ thống thông tin của Quý đơn vị. Để

nắm rõ hơn về những rủi ro tiềm ẩn này, vui lòng tham khảo thông tin chi tiết các lỗ hổng an toàn thông tin xem tại Phụ lục kèm theo.

Nhằm đảm bảo an toàn thông tin, không để tin tặc tận dụng lỗ hổng bảo mật để tiến hành các cuộc vào hệ thống thông tin tập trung của tỉnh, Sở Thông tin và Truyền thông kính đề nghị quý đơn vị chủ động thực hiện các biện pháp sau:

1. Kiểm tra, rà soát, xác định máy tính/máy chủ sử dụng hệ điều hành **Windows** có khả năng bị ảnh hưởng. Thực hiện cập nhật bản vá kịp thời để tránh nguy cơ bị tấn công *(Thông tin chi tiết các lỗ hổng bảo mật có tại phụ lục kèm theo)*.

2. Triển khai cài đặt 02 giải pháp Bkav Endpoint và EDR cho 100% máy tính tại cơ quan, đơn vị theo các hướng dẫn cài đặt của Sở Thông tin và Truyền thông. *Đây là 02 tiêu chí về An toàn thông tin trong Bộ chỉ số đánh giá, xếp hạng Chuyển đổi số các cấp theo Quyết định số 931/QĐ-UBND ngày 04/4/2024 của Ủy ban nhân dân tỉnh Thừa Thiên Huế về việc Quyết định Ban hành Bộ chỉ số đánh giá, xếp hạng chuyển đổi số các cấp của tỉnh Thừa Thiên Huế.*

3. 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 Sở Thông tin và Truyền thông và các cơ quan chức năng về an toàn thông tin để phát hiện kịp thời các nguy cơ tấn công mạng.

4. Rà soát tài khoản, đặt mật khẩu mạnh, thay đổi định kỳ tối thiểu 3 tháng/lần và cử đầu mối thường trực hỗ trợ trong công tác điều phối ứng cứu sự cố.

Trong trường hợp cần hỗ trợ, quý đơn vị liên hệ đầu mối hỗ trợ của Sở Thông tin và Truyền thông:

- đ/c Hoàng Diên Kỷ; điện thoại: 0906 760 759;
email: hdky.stttt@thuathienhue.gov.vn
- đ/c La Thức; điện thoại: 0772 428 218;
email: lthuc.stttt@thuathienhue.gov.vn

Nơi nhận:
- Như trên;
- UBND tỉnh (để bc);
- Công an tỉnh (để p/h);
- BGĐ Sở;
- P.CNTT, HueIOC;
- Lưu: VT.

GIÁM ĐỐC

CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM
SỞ THÔNG TIN VÀ TRUYỀN THÔNG
T. THỪA THIÊN HUẾ

Nguyễn Xuân Sơn

Phụ lục
Thông tin về các lỗ hổng bảo mật Cao và Nghiêm trọng trong sản phẩm Microsoft công bố tháng 9/2024
(Kèm theo Công văn số 2807 /STTTT-IOC ngày 26 /9/2024 của Sở Thông tin và Truyền thông tỉnh Thừa Thiên Huế)

1. Thông tin các lỗ hổng bảo mật

STT	CVE	Mô tả	Link tham khảo
1	CVE-2024-43491	- Điểm CVSS: 9.8 (Nghiêm trọng) - Mô tả: Lỗ hổng trong Microsoft Windows Update cho phép đối tượng tấn công thực thi mã từ xa. Lỗ hổng hiện đang bị khai thác trong thực tế. - Ảnh hưởng: Windows 10.	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-43491
2	CVE-2024-38018 CVE-2024-38227 CVE-2024-38228 CVE-2024-43464	- Điểm CVSS: 8.8 (Nghiêm trọng) - Mô tả: Lỗ hổng trong Microsoft SharePoint Server cho phép đối tượng tấn công thực thi mã từ xa. - Ảnh hưởng: Microsoft SharePoint Server 2019, Microsoft SharePoint Enterprise Server 2016, Microsoft SharePoint Server Subscription Edition.	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38018 https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38227 https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38228 https://msrc.microsoft.com/update-guide/vulnerability/C

STT	CVE	Mô tả	Link tham khảo
			VE-2024-43464
3	CVE-2024-43461	- Điểm CVSS: 8.8 (Cao) - Mô tả: Lỗ hổng trong Windows MSHTML Platform cho phép đối tượng tấn công thực hiện tấn công giả mạo (spoofing). - Ảnh hưởng: Windows 10, Windows 11, Windows Server 2008, 2012, 2016, 2019, 2022.	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-43461
4	CVE-2024-21416 CVE-2024-38045	- Điểm CVSS: 8.1 (Cao) - Mô tả: Lỗ hổng trong Windows TCP/IP 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-2024-21416 https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38045

STT	CVE	Mô tả	Link tham khảo
5	CVE-2024-38014	- Điểm CVSS: 7.8 (Cao) - Mô tả: Lỗ hổng trong Windows Installer cho phép đối tượng tấn công thực hiện leo thang đặc quyền. Lỗ hổng hiện đang bị khai thác trong thực tế. - Ảnh hưởng: Windows 10, Windows 11, Windows Server 2008, 2012, 2016, 2019, 2022.	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38014
6	CVE-2024-43463	- Điểm CVSS: 7.8 (Cao) - Mô tả: Lỗ hổng trong Microsoft Office Visio cho phép đối tượng tấn công thực thi mã từ xa. - Ảnh hưởng: Microsoft Visio 2016, Microsoft Office LTSC 2021, Microsoft 365 Apps for Enterprise, Microsoft Office 2019.	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-43463
7	CVE-2024-38226	- Điểm CVSS: 7.3 (Cao) - Mô tả: Lỗ hổng trong Microsoft Publisher cho phép đối tượng tấn công vượt qua cơ chế bảo vệ. Lỗ hổng hiện đang bị khai thác trong thực tế. - Ảnh hưởng: Microsoft Publisher 2016, Microsoft	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38226

STT	CVE	Mô tả	Link tham khảo
		Office LTSC 2021, Microsoft Office 2019.	
8	CVE-2024-38217 CVE-2024-43487	- Điểm CVSS: 5.4 (Cao) - Mô tả: Lỗ hổng trong Windows Mark of the Web cho phép đối tượng tấn công vượt qua cơ chế bảo vệ. Lỗ hổng hiện đang bị khai thác trong thực tế. - Ảnh hưởng: Windows 10, Windows 11, Windows Server 2008, 2012, 2016, 2019, 2022.	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38217 https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-43487

2. Hướng dẫn khắc phục

Biện pháp tốt nhất để khắc phục là cập nhật bản vá cho các lỗ hổng bảo mật nói trên theo hướng dẫn của hãng. Quý 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/2024/9/10/the-september-2024-security-update-review