

Số: 3087/STTTT-IOC
V/v cảnh báo lỗ hổng bảo mật ảnh hưởng Cao và
Nghiêm trọng trong các sản phẩm Microsoft công
bố tháng 10/2024

Thừa Thiên Huế, ngày 22 tháng 10 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;

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-2024-43468** trong Microsoft Configuration Manager cho phép đối tượng tấn công thực thi mã từ xa.
- Lỗ hổng an toàn thông tin **CVE-2024-43582** trong Remote Desktop Protocol Server cho phép đối tượng tấn công thực thi mã từ xa.
- Lỗ hổng an toàn thông tin **CVE-2024-43572** trong Microsoft Management Console cho phép đối tượng tấn công thực thi mã từ xa. Lỗ hổng hiện đang bị khai thác trong thực tế.
- Lỗ hổng an toàn thông tin **CVE-2024-43583** trong Microsoft Winlogon cho phép đối tượng tấn công thực hiện leo thang đặc quyền. Thông tin chi tiết về lỗ hổng đã được công bố công khai.
- Lỗ hổng an toàn thông tin **CVE-2024-43504** trong Microsoft Excel cho phép đối tượng tấn công thực thi mã từ xa.
- **02** lỗ hổng an toàn thông tin **CVE-2024-43576, CVE-2024-43616** trong Microsoft Office cho phép đối tượng tấn công thực thi mã từ xa.
- Lỗ hổng an toàn thông tin **CVE-2024-43505** trong Microsoft Office Visio cho phép đối tượng tấn công thực thi mã từ xa.
- Lỗ hổng an toàn thông tin **CVE-2024-43573** trong Windows MSHTML Platform cho phép đối tượng tấn công thực hiện tấn công giả mạo (spoofing). 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 Kỳ; điện thoại: 0906 760 759;

email: hdky.stttt@thuathienhue.gov.vn

- đ/c La Thúc; điện thoại: 0772 428 218;

email: ltthuc.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

Nguyễn Xuân Sơn

Phụ lục**Thông tin về các lỗ hổng bảo mật Cao và Nghiêm trọng trong sản phẩm
Microsoft công bố tháng 10/2024**

*(Kèm theo Công văn số 3087/STTTT-IOC ngày 22/10/2024 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-2024-43468	- Điểm CVSS: 9.8 (Nghiêm trọng) - Mô tả: Lỗ hổng trong Microsoft Configuration Manager cho phép đối tượng tấn công thực thi mã từ xa. - Ảnh hưởng: Microsoft Configuration Manager.	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-43468
2	CVE-2024-43582	- Điểm CVSS: 8.1 (Nghiêm trọng) - Mô tả: Lỗ hổng trong Remote Desktop Protocol Server 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-2024-43582
3	CVE-2024-43572	- Điểm CVSS: 7.8 (Cao) - Mô tả: Lỗ hổng trong Microsoft Management Console cho phép đối tượng tấn công thực thi mã từ xa. Lỗ hổng hiện đang bị khai thác trong thực tế.	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-43572

STT	CVE	Mô tả	Link tham khảo
		- Ảnh hưởng: Windows 10, Windows 11, Windows Server 2008, 2012, 2016, 2019, 2022.	
4	CVE-2024-43583	- Điểm CVSS: 7.8 (Cao) - Mô tả: Lỗ hổng trong Microsoft Winlogon cho phép đối tượng tấn công thực hiện leo thang đặc quyền. Thông tin chi tiết về lỗ hổng đã được công bố công khai. - Ảnh hưởng: Windows 10, Windows 11, Windows Server 2008, 2012, 2016, 2019, 2022.	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-43583
5	CVE-2024-43504	- Điểm CVSS: 7.8 (Cao) - Mô tả: Lỗ hổng trong Microsoft Excel cho phép đối tượng tấn công thực thi mã từ xa. - Ảnh hưởng: Microsoft Excel 2016, 2019. Microsoft Office LTSC 2021, 2024. Microsoft 365 Apps for Enterprise.	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-43504
6	CVE-2024-43576 CVE-2024-43616	- 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 2024. Microsoft	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-43576 https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-43616

STT	CVE	Mô tả	Link tham khảo
		365 Apps for Enterprise.	VE-2024-43616
7	CVE-2024-43505	- 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 Office LTSC 2021, 2024. Microsoft 365 Apps for Enterprise, Microsoft Office 2019.	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-43505
8	CVE-2024-43573	- Điểm CVSS: 6.5 (Trung bình) - Mô tả: Lỗ hổng trong Windows MSHTML Platform cho phép đối tượng tấn công thực hiện tấn công giả mạo (spoofing). Lỗ hổng hiện đang bị khai thác trong thực tế. - Ảnh hưởng: Windows 10, Windows 11, Windows Server 2012, 2016, 2019, 2022.	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-43573

2. Hướng dẫn khắc phục

Tăng cường giám sát và sẵn sàng phương án xử lý khi phát hiện có dấu hiệu bị khai thác, tấn công mạng.

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.

Kiểm tra, rà soát, xác định máy tính sử dụng hệ điều hành Windows có khả năng bị ảnh hưởng. 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.

Quý đơn vị tham khảo các bản cập nhật phù hợp cho các sản phẩm đang sử dụng tại link tham khảo mục 1 của Phụ lục.

3. Tài liệu tham khảo

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

<https://www.zerodayinitiative.com/blog/2024/10/8/the-october-2024-security-update-review>