

UBND TỈNH THỪA THIÊN HUẾ
SỞ THÔNG TIN VÀ TRUYỀN THÔNG

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

Số: 690/STTTT-IOC

Thừa Thiên Huế, ngày 21 tháng 3 năm 2024

V/v cảnh báo lỗ hổng bảo mật ảnh hưởng Cao và Nghiêm trọng trong các sản phẩm Microsoft công bố tháng 3/2024

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 12/3/2024, Microsoft đã phát hành danh sách bản vá tháng 3 với **59** 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-2024-26198** trong Microsoft Exchange Server cho phép đối tượng tấn công thực thi mã từ xa.
- Lỗ hổng an toàn thông tin **CVE-2024-21407** trong Windows Hyper-V cho phép đối tượng tấn công thực thi mã từ xa.
- Lỗ hổng an toàn thông tin **CVE-2024-21408** trong Windows Hyper-V cho phép đối tượng tấn công thực hiện tấn công từ chối dịch vụ (DoS).
- Lỗ hổng an toàn thông tin **CVE-2024-21334** trong Open Management Infrastructure (OMI) cho phép đối tượng tấn công thực thi mã từ xa.
- Lỗ hổng an toàn thông tin **CVE-2024-21426** trong Microsoft SharePoint Server cho phép đối tượng tấn công thực thi mã từ xa.
- Lỗ hổng an toàn thông tin **CVE-2024-21411** trong Skype for Consumer cho phép đối tượng tấn công thực thi mã từ xa.

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 2263/QĐ-UBND ngày 27/9/2023 của Ủy ban nhân dân tỉnh Thừa Thiên Huế về việc 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. Hiện nay, qua hệ thống giám sát SOC tại Trung tâm Giám sát, điều hành đô thị thông minh phát hiện nhiều tài khoản bị lộ lọt thông tin trên không gian mạng. Đề nghị Lãnh đạo các cơ quan, đơn vị chỉ đạo CBCCVN trong đơn vị định kỳ thay đổi mật khẩu mạnh 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.sttt@thuathienhue.gov.vn

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

email: lthuc.sttt@thuathienhue.gov.vn

Phòng Giám sát, điều hành an toàn, an ninh mạng - Trung tâm Giám sát, điều hành đô thị thông minh.

Nơi nhận:

- Như trên;
- UBND tỉnh (để bc);
- Công an tỉnh (để p/h);
- Sở Y tế (để p/h);
- Sở GDĐT (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 3/2024

*(Kèm theo Công văn số 690 /STTTT-IOC ngày 21/3/2024 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-2024-26198	<ul style="list-style-type: none">- Điểm: CVSS: 8.8 (Cao)- Mô tả: Lỗ hổng trong Microsoft Exchange Server cho phép đối tượng tấn công thực thi mã từ xa.- Ảnh hưởng: Microsoft Exchange Server 2016, 2019.	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-26198
2	CVE-2024-21407	<ul style="list-style-type: none">- Điểm: CVSS: 8.1 (Nghiêm trọng)- Mô tả: Lỗ hổng trong Windows Hyper-V cho phép đối tượng tấn công thực thi mã từ xa.- Ảnh hưởng: Windows 10, Windows 11; Windows Server 2012, 2012 R2, 2016, 2019, 2022.	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-21407
3	CVE-2024-21408	<ul style="list-style-type: none">- Điểm: CVSS: 5.5 (Nghiêm trọng)- Mô tả: Lỗ hổng trong Windows Hyper-V cho phép đối tượng tấn công thực hiện tấn công từ chối dịch vụ (DoS).- Ảnh hưởng: Windows 10, Windows 11; Windows Server 2016, 2019, 2022.	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-21408

STT	CVE	Mô tả	Link tham khảo
4	CVE-2024-21334	<ul style="list-style-type: none"> - Điểm: CVSS: 9.8 (Cao) - Mô tả: Lỗ hổng trong Open Management Infrastructure (OMI) cho phép đối tượng tấn công thực thi mã từ xa. - Ảnh hưởng: OMI; System Center Operations Manager (SCOM) 2019, 2022. 	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-21334
5	CVE-2024-21426	<ul style="list-style-type: none"> - Điểm: CVSS: 7.8 (Cao) - Mô tả: Lỗ hổng trong Microsoft SharePoint Server cho phép đối tượng tấn công thực thi mã từ xa. - Ảnh hưởng: Microsoft SharePoint Enterprise Server 2016, Microsoft SharePoint Server 2019; Microsoft SharePoint Server Subscription Edition. 	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-21426
6	CVE-2024-21411	<ul style="list-style-type: none"> - Điểm: CVSS: 8.8 (Cao) - Mô tả: Lỗ hổng trong Skype for Consumer cho phép đối tượng tấn công thực thi mã từ xa. - Ảnh hưởng: Skype for Consumer. 	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-21411

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/2024/3/12/the-march-2024-security-update-review>