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: 2608/STTTT-IOC
V/v cảnh báo lỗ hổng bảo mật ảnh hưởng Cao và Nghiêm trọng trong các sản phẩm Microsoft công bố tháng 11/2022

Thừa Thiên Huế, ngày 15 tháng 11 năm 2022

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 08/11/2022, Microsoft đã phát hành danh sách bản vá tháng 11 với 64 lỗ hổng bảo mật trong các sản phẩm của mình. Bản phát hành tháng này đặc biệt đáng chú ý các lỗ hổng bảo mật có mức ảnh hưởng cao và nghiêm trọng sau:

- 06 lỗ hổng bảo mật **CVE-2022-41082, CVE-2022-41040, CVE-2022-41080, CVE-2022-41079, CVE-2022-41078, CVE-2022-41123** trong Microsoft Exchange Server cho phép đối tượng tấn công thực thi mã từ xa, nâng cao đặc quyền. Trong đó, 02 lỗ hổng CVE-2022-41082, CVE-2022-41040 đã được cảnh báo tại văn bản số 1484/CATTT-VNCERT/CC về việc cảnh báo lỗ hổng bảo mật zero-day ảnh hưởng nghiêm trọng đến Microsoft Exchange phát hành ngày 30/9/2022.

- 02 lỗ hổng bảo mật **CVE-2022-41128, CVE-2022-41118** trong Windows Scripting Languages cho phép đối tượng tấn công thực thi mã từ xa. Lỗ hổng này đang bị khai thác trong thực tế.

- Lỗ hổng bảo mật **CVE-2022-41091** trong Windows Mark of the Web cho phép đối tượng tấn công thực hiện tấn công vượt qua cơ chế bảo mật.

- Lỗ hổng bảo mật **CVE-2022-41073** trong Windows Print Spooler cho phép đối tượng tấn công thực hiện tấn công nâng cao đặc quyền.

- Lỗ hổng bảo mật **CVE-2022-41125** trong Windows CNG Key Insolation Service cho phép đối tượng tấn công thực hiện tấn công nâng cao đặc quyền.

- 03 lỗ hổng bảo mật **CVE-2022-41044, CVE-2022-41088, CVE-2022-41039** trong Windows Point-to-Point cho phép đối tượng tấn công thực thi mã từ xa.

- 04 lỗ hổng bảo mật **CVE-2022-41105, CVE-2022-41106, CVE-2022-41063, CVE-2022-41104** trong Microsoft Excel cho phép đối tượng tấn công thực thi mã từ xa, tấn công giả mạo (Spoofing), thực hiện tấn công vượt qua cơ chế bảo mật.

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 Văn bản số 639/STTTT-IOC ngày 29/3/2022 về việc triển khai giải pháp phòng, chống mã độc tập trung BKAV Endpoint cho toàn bộ cơ quan nhà nước trên địa bàn tỉnh và Văn bản số 1660/STTTT-IOC ngày 22/7/2022 về việc triển khai giải pháp phát hiện và chống tấn công có chủ đích Viettel Endpoint.

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.

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

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

Trân trọng./.

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 11/2022
(Kèm theo Công văn số /STTTT-IOC ngày /11/2022 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-2022-41082, CVE-2022-41040, CVE-2022-41080, CVE-2022-41079, CVE-2022-41078, CVE-2022-41123	- Điểm CVSS: 8.8 (Cao) - Lỗ hổng trong Microsoft Exchange Server cho phép đối tượng tấn công thực thi mã từ xa, nâng cao đặc quyền. - Ảnh hưởng: Microsoft Exchange Server 2016 CU 23/22, Exchange Server 2019 CU 11, Exchange Server 2013 CU 23	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-41082 https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-41040 https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-41080 https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-41123 https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-41078 https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-41079
2	CVE-2022-41128, CVE-2022-41118	- Điểm CVSS: 8.8 (Cao) - Lỗ hổng trong trong Windows Scripting Languages cho phép đối tượng tấn công thực thi mã từ xa. Lỗ hổng này	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-41128 https://msrc.microsoft.com/update-

STT	CVE	Mô tả	Link tham khảo
		đang bị khai thác trong thực tế. - Ảnh hưởng: Windows Server 2008/2012/2016/2019/2022, Windows 11/10/8.1/7.	guide/vulnerability/CVE-2022-41118
3	CVE-2022-41091	- Điểm CVSS: 5.4 (Trung bình) - Lỗ hổng trong Windows Mark of the Web cho phép đối tượng tấn công thực hiện tấn công vượt qua cơ chế bảo mật. - Ảnh hưởng: Windows 10/11, Windows Server 2016/2019/2022.	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-41091
4	CVE-2022-41073	- Điểm CVSS: 7.8 (Cao) - Lỗ hổng Windows Print Spooler cho phép đối tượng tấn công thực hiện tấn công nâng cao đặc quyền. - Ảnh hưởng: Windows Server 2008/2012/2016/2019/2022, Windows 11/10/8.1/7.	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-41073
5	CVE-2022-41125	- Điểm CVSS: 7.8 (Cao) - Lỗ hổng Windows CNG Key Insolation Service cho phép đối tượng tấn công thực hiện tấn công nâng cao đặc quyền.	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-41125

STT	CVE	Mô tả	Link tham khảo
		- Ảnh hưởng: Windows 8.1/10/11, Windows Server 2012/2016/2019/2022	
6	CVE-2022-41044, CVE-2022-41088, CVE-2022-41039	- Điểm CVSS: 8.1 (Cao) - Lỗ hổng trong Windows Point-to-Point cho phép đối tượng tấn công thực thi mã từ xa. - Ảnh hưởng: Windows 8.1/10/11, Windows Server 2012/2016/2019.	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-41044 https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-41088 https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-41039
7	CVE-2022-41105, CVE-2022-41106, CVE-2022-41063, CVE-2022-41104	- Điểm CVSS: 7.8 (Cao) - Lỗ hổng trong Microsoft Excel cho phép đối tượng tấn công thực thi mã từ xa, tấn công giả mạo (Spoofing), thực hiện tấn công vượt qua cơ chế bảo mật. - Ảnh hưởng: Microsoft Excel 2013/2016, Microsoft Office, Microsoft 365.	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-41105 https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-41106 https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-41063 https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-41104

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/releaseNote/2022-Nov

https://www.zerodayinitiative.com/blog/2022/11/8/the-november-2022-security-update-review