

Số: /STTTT-BCVTCNTT

Lai Châu, ngày tháng năm 2022

V/v Cảnh báo lỗ hổng bảo mật ảnh hưởng
cao và nghiêm trọng trong các sản phẩm
Microsoft công bố tháng 11/2022

Kính gửi:

- Các Sở, Ban, Ngành tỉnh;
- UBND các huyện, thành phố.

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 Isolation 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.

Thông tin chi tiết các lỗ hổng bảo mật có tại phụ lục kèm theo.

Nhằm đảm bảo an toàn thông tin cho hệ thống thông tin của Quý cơ quan, góp phần bảo đảm an toàn cho không gian mạng Việt Nam, Sở Thông tin và Truyền thông đề nghị quý cơ quan thực hiện:

1. Kiểm tra, rà soát, xác định máy 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 (*Tham khảo thông tin tại phụ lục kèm theo*).

2. 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 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.

3. Trường hợp cần thiết, báo cáo về Sở Thông tin và Truyền thông theo số điện thoại: 02133798798 hoặc đầu mối hỗ trợ của Cục An toàn thông tin: Trung tâm Giám sát an toàn không gian mạng quốc gia, điện thoại 02432091616 để có biện pháp khắc phục, xử lý kịp thời.

Trên đây là cảnh báo lỗ hổng bảo mật ảnh hưởng cao và nghiêm trọng trong các sản phẩm Microsoft công bố tháng 11/2022, kính đề nghị Quý cơ quan quan tâm thực hiện./.

Nơi nhận:

- Như trên;
- Lưu: VT, BCVTCNTT.

GIÁM ĐỐC

Nguyễn Minh Hiệu

PHỤ LỤC

Thông tin về các lỗ hổng bảo mật trong sản phẩm Microsoft tháng 11/2022
(Kèm theo công văn số /STTTT-BCVTCNTT ngày tháng năm 2022)

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	<ul style="list-style-type: none"> - 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-2022-41079 https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-41078 https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-41123
2	CVE-2022-41128, CVE-2022-41118	<ul style="list-style-type: none"> - Điểm CVSS: 8.8 (Cao) - Lỗ hổng 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. - Ảnh hưởng: Windows Server 2008/2012/2016/2019/2022, Windows 11/10/8.1/7. 	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-41128 https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-41118
3	CVE-2022-41091	<ul style="list-style-type: none"> - Điểm CVSS: 5.4 (Trung bình) 	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-41091

		<ul style="list-style-type: none"> - 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. 	guide/vulnerability/CVE-2022-41091
4	CVE-2022-41073	<ul style="list-style-type: none"> - 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	<ul style="list-style-type: none"> - 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. - Ảnh hưởng: Windows 8.1/10/11, Windows Server 2012/2016/2019/2022 	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-41125
6	CVE-2022-41044, CVE-2022-41088, CVE-2022-41039	<ul style="list-style-type: none"> - 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	<ul style="list-style-type: none"> - 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>