

Số: /CATT-NCSC
V/v lỗ hổng an toàn thông tin ảnh hưởng
cao và nghiêm trọng trong các sản phẩm
Microsoft công bố tháng 10/2023

Hà Nội, ngày tháng năm 2023

Kính gửi:

- Đơn vị chuyên trách về CNTT các Bộ, cơ quan ngang Bộ, cơ quan thuộc Chính phủ;
- Sở Thông tin và Truyền thông các tỉnh, thành phố trực thuộc Trung ương;
- Các Tập đoàn, Tổng công ty nhà nước; các Ngân hàng TMCP; các tổ chức tài chính;
- Hệ thống các đơn vị chuyên trách về an toàn thông tin.

Ngày 10/10/2023, Microsoft đã phát hành danh sách bản vá tháng 10 với 103 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-2023-36778** trong Microsoft Exchange Server cho phép đối tượng tấn công thực thi mã từ xa.

Trung tâm Giám sát an toàn không gian mạng quốc gia (NCSC), Cục An toàn thông tin, đã phát hành các văn bản cảnh báo diện rộng về những lỗ hổng ảnh hưởng đến Microsoft Exchange Server. Điều này cho thấy Microsoft Exchange Server vẫn luôn là mục tiêu hàng đầu được các đối tượng tấn công có chủ đích nhắm đến. Vì vậy, để đảm bảo an toàn thông tin cho hệ thống của các cơ quan, tổ chức, Cục An toàn thông tin trân trọng đề nghị các đơn vị rà soát lỗ hổng liên quan đến Microsoft Exchange Server để phát hiện và có phương án xử lý kịp thời, đồng thời tăng cường giám sát nhằm giảm thiểu nguy cơ bị tấn công thông qua các lỗ hổng này.

- Lỗ hổng an toàn thông tin **CVE-2023-36563** trong Microsoft WordPad cho phép đối tượng tấn công thực hiện thu thập thông tin mã băm NTLM của người dùng. Lỗ hổng hiện đang bị khai thác trong thực tế.

- Lỗ hổng an toàn thông tin **CVE-2023-41763** trong Skype for Business cho phép đối tượng tấn công thực hiện leo thang đặc quyền. Lỗ hổng hiện đang bị khai thác trong thực tế.

- 02 lỗ hổng an toàn thông tin **CVE-2023-35349**, **CVE-2023-36697** trong Microsoft Message Queuing cho phép đối tượng tấn công thực thi mã từ xa.

- Lỗ hổng an toàn thông tin **CVE-2023-36434** trong Windows IIS Server

cho phép đối tượng tấn công thực hiện leo thang đặc quyền.

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 đơn vị, góp phần bảo đảm an toàn cho không gian mạng Việt Nam, Cục An toàn thông tin khuyến nghị Quý đơn vị thực hiện:

1. Kiểm tra, rà soát, xác định máy tính 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. Trong trường hợp cần thiết có thể liên hệ đầu mối hỗ trợ của Cục An toàn thông tin: Trung tâm Giám sát an toàn không gian mạng quốc gia, điện thoại 02432091616, thư điện tử: ncsc@ais.gov.vn.

Trân trọng./.

Nơi nhận:

- Như trên;
- Bộ trưởng (đề b/c);
- Thứ trưởng Nguyễn Huy Dũng (đề b/c);
- Cục A05, Bộ Công an;
- Bộ Tư lệnh 86, Bộ Quốc phòng;
- Ban Cơ yếu Chính phủ;
- Đơn vị chuyên trách về ATTT của: Văn phòng Trung ương Đảng; Văn phòng Quốc hội; Văn phòng Chủ tịch nước; Tòa án Nhân dân tối cao; Viện Kiểm sát Nhân dân tối cao;
- Các Cục: Viễn thông, Bưu điện Trung ương;
- Các Trung tâm: TTTT, VNNIC;
- Cục trưởng (đề b/c);
- Các Phó Cục trưởng;
- P. ATHTTT, VNCERT/CC;
- Lưu: VT, NCSC.LTQ.

**KT. CỤC TRƯỞNG
PHÓ CỤC TRƯỞNG**

Trần Đăng Khoa

Phụ lục
THÔNG TIN VỀ CÁC LỖ HỔNG AN TOÀN THÔNG TIN
TRONG SẢN PHẨM MICROSOFT

(Kèm theo Công văn số /CATTT-NCSC
ngày / /2023 của Cục An toàn thông tin)

1. Thông tin các lỗ hổng an toàn thông tin

STT	CVE	Mô tả	Link tham khảo
1	CVE-2023-36778	<ul style="list-style-type: none"> - Điểm: CVSS: 8.0 (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-2023-36778
2	CVE-2023-36563	<ul style="list-style-type: none"> - Điểm: CVSS: 6.5 (Cao) - Mô tả: Lỗ hổng trong Microsoft WordPad cho phép đối tượng tấn công thực hiện thu thập thông tin mã băm NTLM của người dùng. 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-2023-36563
3	CVE-2023-41763	<ul style="list-style-type: none"> - Điểm: CVSS: 5.3 (Cao) - Mô tả: Lỗ hổng trong Skype for Business cho phép đối tượng tấn công thực hiện leo thang đặc quyền. Lỗ hổng hiện đang bị khai thác trong thực tế. - Ảnh hưởng: Skype for Business 2015, 2019. 	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-41763
		<ul style="list-style-type: none"> - Điểm: CVSS: 9.8 (Nghiêm trọng) 	https://msrc.microsoft.com/update-

STT	CVE	Mô tả	Link tham khảo
4	CVE-2023-35349 CVE-2023-36697	- Mô tả: Lỗ hổng trong Microsoft Message Queuing cho phép đối tượng tấn công thực thi mã từ xa. - Ảnh hưởng: Windows 10, Windows 11, Windows Server 2008, 2012, 2016, 2019, 2022.	guide/vulnerability/CVE-2023-35349 https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-36697
5	CVE-2023-36434	- Điểm: CVSS: 9.8 (Cao) - Mô tả: Lỗ hổng trong Windows IIS Server cho phép đối tượng tấn công thực hiện leo thang đặc quyền. - Ảnh hưởng: Windows 10, Windows 11, Windows Server 2008, 2012, 2016, 2019, 2022	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-36434

2. Hướng dẫn khắc phục

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 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/2023/10/10/the-october-2023-security-update-review>