

Số: /CATTT-NCSC
V/v lỗ hổng bảo mật ảnh hưởng cao và
nghiêm trọng trong các sản phẩm
Microsoft công bố tháng 05/2023

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 09/05/2023, Microsoft đã phát hành danh sách bản vá tháng 05 với 38 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:

- Lỗ hổng bảo mật **CVE-2023-24955** trong Microsoft SharePoint Server cho phép đối tượng tấn công thực thi mã từ xa.

Trong tháng 01 vừa qua, đã có hai lỗ hổng bảo mật được công bố với mã là CVE-2023-21744, CVE-2023-21742 liên quan đến Microsoft SharePoint Server, những lỗ hổng này cho phép đối tượng tấn công thực thi mã từ xa, đã được Trung tâm Giám sát an toàn không gian mạng quốc gia (NCSC) cảnh báo trong văn bản số 50/CATTT-NCSC về việc lỗ hổng bảo mật ảnh hưởng cao và nghiêm trọng trong các sản phẩm Microsoft công bố tháng 01/2023 phát hành ngày 11/01/2023. Qua đó cho thấy, Microsoft SharePoint Server đã và đang là mục tiêu nhắm đến của nhiều đối tượng tấn công mạng nhằm thực hiện các hành động trái phép. Chính vì vậy, các cơ quan, tổ chức cần đặc biệt quan tâm và có phương án khắc phục, xử lý kịp thời nếu bị ảnh hưởng.

- 02 lỗ hổng bảo mật **CVE-2023-29336, CVE-2023-24902** trong Win32k cho phép đối tượng tấn công thực hiện tấn công nâng cao đặc quyền. Lỗ hổng này đang bị khai thác trong thực tế.

- Lỗ hổng bảo mật **CVE-2023-29325** trong Windows OLE cho phép đối tượng tấn công thực thi mã từ xa. Lỗ hổng này đã được công bố rộng rãi trên Internet.

- Lỗ hổng bảo mật **CVE-2023-24941** trong Windows Network File System cho phép đối tượng tấn công thực thi mã từ xa.

- Lỗ hổng bảo mật **CVE-2023-24932** trong Secure Boot cho phép đối tượng tấn công thực hiện tấn công vượt qua cơ chế bảo mật (Bypass). Lỗ hổng này đã được công bố rộng rãi trên Internet.

- Lỗ hổng bảo mật **CVE-2023-29344** trong Microsoft Office cho phép đối tượng tấn công thực thi mã từ xa.

- Lỗ hổng bảo mật **CVE-2023-24953** trong Microsoft Excel cho phép đối tượng tấn công thực thi mã từ xa.

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 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: ais@mic.gov.vn.

Trân trọng./.

Nơi nhận:

- Như trên;
- Bộ trưởng (để b/c);
- Thứ trưởng Nguyễn Huy Dũng (để b/c);
- Cục A05, Bộ Công an;
- Bộ Tư lệnh 86, Bộ Quốc phòng;
- Ban Cơ yếu Chính phủ;
- Cục trưởng (để b/c);
- Các Phó Cục trưởng;
- Trung tâm VNCERT/CC, Phòng ATHTTT;
- Lưu: VT, NCSC.

**KT. CỤC TRƯỞNG
PHÓ CỤC TRƯỞNG**

Trần Đăng Khoa

Phụ lục
THÔNG TIN VỀ CÁC LỖ HỔNG BẢO MẬT TRONG
SẢN PHẨM MICROSOFT

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

1. Thông tin các lỗ hổng bảo mật

STT	CVE	Mô tả	Link tham khảo
1	CVE-2023-24955	- Điểm: CVSS: 7.2 (cao) - Mô tả: lỗ hổng trong Microsoft SharePoint Server cho phép đối tượng tấn công thực thi mã từ xa. - Ảnh hưởng: Microsoft SharePoint Server.	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-24955
2	CVE-2023-29336 CVE-2023-24902	- Điểm: CVSS: 7.8 (cao) - Mô tả: lỗ hổng trong Win32k cho phép đối tượng tấn công thực hiện tấn công nâng cao đặc quyền. Lỗ hổng này đang bị khai thác trong thực tế. - Ảnh hưởng: Windows Server, Windows 10,11.	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-29336 https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-24902
3	CVE-2023-29325	- Điểm: CVSS: 8.1 (cao) - Mô tả: lỗ hổng trong Windows OLE cho phép đối tượng tấn công thực thi mã từ xa. Lỗ hổng này đã được công bố rộng rãi trên Internet. - Ảnh hưởng: Windows Server, Windows 10/11.	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-29325
4	CVE-2023-24941	- Điểm: CVSS: 9.8 (nghiêm trọng) - Mô tả: lỗ hổng trong Windows Network File System cho phép đối tượng tấn công thực thi mã từ xa. - Ảnh hưởng: Windows Server.	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-24941
5	CVE-2023-24932	- Điểm: CVSS: 6.7 (trung bình) - Mô tả: lỗ hổng trong Secure Boot cho phép đối	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-24932

		<p>tượng tấn công thực hiện tấn công vượt qua cơ chế bảo mật (Bypass). Lỗ hổng này đã được công bố rộng rãi trên Internet.</p> <ul style="list-style-type: none"> - Ảnh hưởng: Windows Server, Windows 10/11. 	
6	CVE-2023-29344	<ul style="list-style-type: none"> - 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, Microsoft 365. 	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-29344
7	CVE-2023-24953	<ul style="list-style-type: none"> - 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 Office, Microsoft 365, Microsoft Excel. 	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-24953

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/2023/5/8/the-may-2023-security-update-review>