

Số: /CATT-NCSC
V/v lỗ hổng bảo mật ảnh hưởng cao
và nghiêm trọng trong các sản phẩm
Microsoft công bố tháng 02/2023

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 14/02/2023, Microsoft đã phát hành danh sách bản vá tháng 02 với 75 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:

- 04 lỗ hổng bảo mật **CVE-2023-21529, CVE-2023-21710, CVE-2023-21707, CVE-2023-21706** trong Microsoft Exchange Server cho phép đối tượng tấn công thực thi mã từ xa. Microsoft Exchange Server đã và đang là mục tiêu hàng đầu được các nhóm tấn công có chủ đích (APT) nhắm đến, các đối tượng tấn công khai thác triệt để. Vì vậy, các cơ quan, tổ chức cần đặc biệt chú ý cũng như có kế hoạch để khắc phục và tăng cường giám sát nhằm giảm thiểu và tránh nguy cơ bị tấn công thông qua các lỗ hổng này.

- Lỗ hổng bảo mật **CVE-2023-21716** trong Microsoft Word cho phép đối tượng tấn công thực thi mã từ xa.

- Lỗ hổng bảo mật **CVE-2023-21715** trong Microsoft Publisher cho phép đối tượng tấn công thực hiện tấn công vượt qua cơ chế bảo mật (Bypass). Lỗ hổng này đang bị khai thác trong thực tế.

- 02 lỗ hổng bảo mật **CVE-2023-23376, CVE-2023-21812** trong Windows Common Log File System (CLFS) cho phép đối tượng tấn công thực hiện tấn công nâng cao đặc quyền. Lỗ hổng này đang bị khai thác trong thực tế.

- 03 lỗ hổng bảo mật **CVE-2023-21705, CVE-2023-21713, CVE-2023-21528** trong Microsoft SQL Server cho phép đối tượng tấn công thực thi mã từ xa.

- Lỗ hổng bảo mật **CVE-2023-21717** trong Microsoft SharePoint Server cho phép đối tượng tấn công thực hiện nâng cao 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 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, P.ATHTTT;
- Lưu: VT, NCSC.

**KT. CỤC TRƯỞNG
PHÓ CỤC TRƯỞNG**

Trần Đăng Khoa

Phụ lục
THÔNG TIN VỀ CÁC LỖ HỒNG 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 hồng bảo mật

STT	CVE	Mô tả	Link tham khảo
1	CVE-2023-21529, CVE-2023-21710, CVE-2023-21707, CVE-2023-21706	<ul style="list-style-type: none"> - Điểm: CVSS: 8.8/7.2 (cao) - Mô tả: lỗ hồng trong Microsoft Exchange Server cho phép đối tượng tấn công thực thi mã từ xa. - Ảnh hưởng: Microsoft Exchange Server. 	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-21529 https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-21706 https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-21710 https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-21707
2	CVE-2023-21716	<ul style="list-style-type: none"> - Điểm: CVSS: 9.8 (nghiêm trọng) - Mô tả: lỗ hồng trong Microsoft Word cho phép đối tượng tấn công thực thi mã từ xa. - Ảnh hưởng: Microsoft Word, Microsoft SharePoint. 	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-21716
3	CVE-2023-21715	<ul style="list-style-type: none"> - Điểm: CVSS: 7.3 (cao) - Mô tả: lỗ hồng trong Microsoft Publisher cho phép đối tượng tấn công thực hiện tấn công vượt qua cơ chế bảo mật (Bypass). Lỗ hồng này đang bị khai thác trong thực tế. - Ảnh hưởng: Microsoft 365. 	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-21715

4	CVE-2023-23376, CVE-2023-21812	<ul style="list-style-type: none"> - Điểm: CVSS: 7.8 (cao) - Mô tả: lỗ hổng trong Windows Common Log File System (CLFS) 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 10/11, Windows Server. 	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-23376 https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-21812
5	CVE-2023-21705, CVE-2023-21713, CVE-2023-21528	<ul style="list-style-type: none"> - Điểm: CVSS: 8.8/7.8 (cao) - Mô tả: lỗ hổng trong Microsoft SQL Server cho phép đối tượng tấn công thực thi mã từ xa. - Ảnh hưởng: SQL Server. 	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-21705 https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-21713 https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-21528
6	CVE-2023-21717	<ul style="list-style-type: none"> - Điểm: CVSS: 8.8 (cao) - Mô tả: lỗ hổng trong Microsoft SharePoint Server cho phép đối tượng tấn công thực hiện nâng cao đặc quyền. - Ảnh hưởng: Microsoft SharePoint. 	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-21717

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/2023/2/14/the-february-2023-security-update-overview>