

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

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

1. Thông tin các lỗ hỏng 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 hỏng 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 hỏng 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 hỏng trong Microsoft Publisher cho phép đối tượng tấn công thực hiện tấn công vượt qua cơ chế bảo mật (Bypass). Lỗ hỏng 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>