BỘ GIAO THÔNG VẬN TẢI
TRUNG TÂM CÔNG NGHỆ THÔNG TIN

CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM
Độc lập - Tự do - Hạnh phúc

Số: 11 /TTCNTT-HT
V/v cảnh báo các lỗ hổng bảo mật tháng 01/2023

Hà Nội, ngày 16 tháng 01 năm 2023

Kính gửi: Các cơ quan, đơn vị, doanh nghiệp trực thuộc Bộ

Trung tâm Công nghệ thông tin nhận được thông tin cảnh báo từ các cơ quan chức năng về nguy cơ tấn công mạng liên quan tới các lỗ hổng bảo mật trong các sản phẩm của Microsoft (Windows Advanced Local Procedure Call (ALPC), Microsoft SharePoint Server, Microsoft Exchange Server, Windows Workstation Service, Microsoft Cryptographic Services, Microsoft Office). Các lỗ hổng bảo mật này cho phép đối tượng tấn công thực thi mã từ xa.

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

Để đảm bảo an toàn thông tin mạng cho các hệ thống, Trung tâm Công nghệ thông tin đề nghị các đơn vị chủ động thực hiện các biện pháp sau:

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.

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.

Trường hợp cần thiết, liên hệ với Trung tâm Công nghệ thông tin (điện thoại: 0985366388) và các cơ quan chức năng về an toàn, an ninh mạng để xử lý./.

Nơi nhận:
- Như trên;
- Giám đốc (để b/c);
- Các Phòng: HT-ATTT, PM (để thực hiện);
- Lưu: VT, HT (TrungDĐ).

KT. GIÁM ĐỐC
PHÓ GIÁM ĐỐC

BỘ GIAO THÔNG VẬN TẢI
TRUNG TÂM CÔNG NGHỆ THÔNG TIN

Phùng Văn Trọng

PHỤ LỤC

Thông tin về các lỗ hổng bảo mật trong sản phẩm Microsoft

(Kèm theo Văn bản số 11 */TTCNTT-HT ngày16 /01/2023 của Trung CNTT)*

1. Thông tin các lỗ hổng bảo mật

STT	CVE	Mô tả	Link tham khảo
1	CVE-2023-21674	- Điểm: CVSS: 8.8 (cao) - Mô tả: lỗ hổng trong Windows Advanced Local Procedure Call (ALPC) cho phép đối tượng tấn công thực hiện nâng cao đặc quyền. Lỗ hổng này đang bị khai thác trong thực tế. - Ảnh hưởng: Windows 8.1/10/11, Windows Server 2012/2019/2022.	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-21674
2	CVE-2023-21743, CVE-2023-21744, CVE-2023-21742	- Điểm: CVSS: 8.8 (cao) - Mô tả: lỗ hổng trong trong Microsoft SharePoint Server cho phép đối tượng tấn công thực hiện tấn công vượt qua cơ chế bảo mật (Bypass), thực thi mã từ xa. - Ảnh hưởng: Windows 8.1/10/11, Windows Server 2012/2019/2022.	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-21743 https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-21744 https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-21742
3	CVE-2023-21763, CVE-2023-21764, CVE-2023-21762, CVE-2023-21745	- Điểm: CVSS: 8.0/7.8 (cao) - Mô tả: lỗ hổng trong trong Microsoft Exchange Server cho phép đối tượng tấn công thực hiện nâng cao đặc quyền, tấn công giả mạo (Spoofing). - Ảnh hưởng: Microsoft Exchange Server 2016/2019.	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-21763 https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-21764 https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-21762 https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-21745
4	CVE-2023-21549	- Điểm: CVSS: 8.8 (cao) - Mô tả: lỗ hổng trong Windows Workstation Service cho phép đối tượng tấn công thực hiện nâng cao đặc quyền. Lỗ hổng này đã được công bố rộng rãi trên Internet. - Ảnh hưởng: Windows 7/8.1/10/11, Windows Server 2012/2019/2022.	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-21549

STT	CVE	Mô tả	Link tham khảo
5	CVE-2023-21561, CVE-2023-21551	- Điểm: CVSS: 8.8/7.8 (cao) - Mô tả: lỗ hổng trong Microsoft Cryptographic Services cho phép đối tượng tấn công thực hiện nâng cao đặc quyền. - Ảnh hưởng: Windows 7/8.1/10/11, Windows Server 2008/2012/2016/2019/ 2022.	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-21561 https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-21551
6	CVE-2023-21734, CVE-2023-21735	- 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 LTSC for Mac 2021, Microsoft 365, Microsoft Office 2019 for Mac.	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-21734 https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-21735

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 của phụ lục.

3. Tài liệu tham khảo

https://msrc.microsoft.com/update-guide

https://www.zerodayinitiative.com/blog/2023/1/10/the-january-2023-security-update-review