BỘ VĂN HÓA, THỂ THAO VÀ DU LỊCH
TRUNG TÂM CÔNG NGHỆ THÔNG TIN

Số: 360 /CV-CNTT

V/v cảnh báo lỗ hổng bảo mật ảnh hưởng cao và nghiêm trọng trong các sản phẩm Microsoft công bố tháng 06/2023

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

Hà Nội, ngày 26 tháng 06 năm 2023

Kính gửi: Các cơ quan hành chính, đơn vị sự nghiệp thuộc Bộ

Cục An toàn thông tin - Bộ Thông tin và Truyền thông tin có văn bản số 1024/CATTT-NCSC ngày 21/06/2023 về việc cảnh báo lỗ hổng bảo mật ảnh hưởng cao và nghiêm trọng trong các sản phẩm Microsoft công bố tháng 06/2023 và đã phát hành bản vá với 69 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 sau: CVE-2023-32031, CVE-2023-28310, CVE-2023-29357, CVE-2023-33142, CVE-2023-29363, CVE-2023-32014, CVE-2023-32015, CVE-2023-3079, CVE-2023-32029, CVE-2023-33133, CVE-2023-33137, CVE-2023-33146.

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, Trung tâm Công nghệ thông tin đề nghị Quý đơn vị triển khai quyết liệt một số khuyến nghị sau:

1. Kiểm tra, rà soát, xác định máy sử dụng hệ điều hành Windows có khả năng bị ảnh hưởng bởi lỗ hổng nêu trên, thực hiện cập nhật bản vá kịp thời để tránh nguy cơ bị tấn công. *(Thông tin chi tiết các lỗ hổng bảo mật có tại phụ lục kèm theo)*.

2. Tăng cường theo dõi, giám sát hệ thống và sẵn sàng phương án xử lý khi phát hiện có dấu hiệu bị khai thác, tấn công mạng.

Trong trường hợp cần hỗ trợ xử lý, đề nghị liên hệ đầu mối kỹ thuật của Trung tâm Công nghệ thông tin: Đ/c Dương Anh Quân - Phòng Quản lý hạ tầng & Dữ liệu số, điện thoại 0915.091.580, thư điện tử: quanda@cntt.gov.vn.

Trân trọng./.

Nơi nhận:
- Như trên;
- Thứ trưởng Hoàng Đạo Cương *(để báo cáo);*
- Giám đốc *(để báo cáo)*;
- Lưu: VT, QLHTDLS, N.80

KT. GIÁM ĐỐC
PHÓ GIÁM ĐỐC

BỘ VĂN HÓA THỂ THAO VÀ DU LỊCH
TRUNG TÂM CÔNG NGHỆ THÔNG TIN

Nguyễn Xuân Thềm

BỘ VĂN HÓA, THỂ THAO VÀ DU LỊCH
TRUNG TÂM CÔNG NGHỆ THÔNG TIN

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

Phụ lục
Thông tin về các lỗ hổng bảo mật trong sản phẩm Microsoft
(Kèm theo Công văn số: /CV-CNTT, ngày tháng năm 2023 của Trung tâm Công nghệ thông tin)

1. Thông tin các lỗ hổng bảo mật

STT	CVE	Mô tả	Link tham khảo
1	CVE-2023-32031 CVE-2023-28310	- Điểm: CVSS: 8.8 (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-2023-32031. https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-28310.
2	CVE-2023-29357 CVE-2023-33142	- Điểm: CVSS: 9.8 (Nghiêm trọng). - Mô tả: lỗ hổng trong Microsoft SharePoint Server cho phép đối tượng tấn công thực hiện nâng cao đặc quyền. - Ảnh hưởng: Microsoft SharePoint Server 2019	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-29357. https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-33142.
3	CVE-2023-29363 CVE-2023-32014 CVE-2023-32015	- Điểm: CVSS: 9.8 (Nghiêm trọng) - Mô tả: lỗ hổng trong Windows Pragmatic General Multicast (PGM) cho phép đối tượng tấn công thực thi mã từ xa. - Ảnh hưởng: Windows Server, Windows 10/11.	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-29363 https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-32014 https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-32015
4	CVE-2023-3079	- Điểm: CVSS: N/A - Mô tả: lỗ hổng trong JavaScript V8 cho phép đối tượng tấn công có thể thực thi các đoạn mã với quyền của người dùng cục bộ. Lỗ hổng này đang bị khai thác trong thực tế. - Ảnh hưởng: Microsoft Edge (Chromium-based)	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-3079

5	CVE-2023-32029 CVE-2023-33133 CVE-2023-33137	- 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 Excel, Microsoft Office.	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-32029 https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-33133 https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-33137
6	CVE-2023-33146	- 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-2023-33146

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/2023/6/13/the-june-2023-security-update- review.