BỘ THÔNG TIN TRUYỀN THÔNG
CỤC AN TOÀN THÔNG TIN

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

Số: 554 /CATTT-NCSC
V/v lỗ hổng bảo mật ảnh hưởng cao và nghiêm trọng trong các sản phẩm Microsoft công bố tháng 04/2023

Hà Nội, ngày 17 tháng 04 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 11/04/2023, Microsoft đã phát hành danh sách bản vá tháng 04 với 97 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-2023-28252** trong Windows Common Log File System Driver 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-2023-21554** trong Microsoft Message Queuing cho phép đối tượng tấn công thực thi mã từ xa.

- 03 lỗ hổng bảo mật **CVE-2023-23384, CVE-2023-23375, CVE-2023-28304** trong Microsoft SQL Server cho phép đối tượng tấn công thực thi mã từ xa.

- Lỗ hổng bảo mật **CVE-2013-3900** xác thực chữ ký WinVerifyTrust cho phép đối tượng tấn công có thể thêm nội dung vào phần chữ ký mã xác thực trong tệp thực thi đã ký mà không làm mất hiệu lực chữ ký. Gần đây, lỗ hổng này đã được sử dụng trong các cuộc tấn công chuỗi cung ứng vào phần mềm của hãng 3CX. Microsoft đã đưa ra bản vá về việc kiểm tra tính xác thực của chữ ký dưới dạng tùy chọn bật hoặc tắt, nếu không được cấu hình sẽ mặc định là tắt. Trong bản cập nhật này Microsoft đã bổ sung thêm các phiên bản hệ điều hành bị ảnh hưởng. Để nâng cao bảo mật an toàn thông tin cho các thiết bị sử dụng hệ điều hành Windows người dùng có thể xem xét việc bật tùy chọn kiểm tra này.

- 02 lỗ hổng bảo mật **CVE-2023-28287, CVE-2023-28295** trong Microsoft Publisher cho phép đối tượng tấn công thực thi mã từ xa.

- 02 lỗ hổng bảo mật **CVE-2023-28309, CVE-2023-28314** trong Microsoft

Dynamics 365 cho phép đối tượng tấn công thực hiện tấn công XSS.

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

CỘNG HÒA X.H.C.N VIỆT NAM
CỤC AN TOÀN THÔNG TIN
BỘ THÔNG TIN VÀ TRUYỀN THÔNG

Trần Đăng Khoa

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 hổng bảo mật

STT	CVE	Mô tả	Link tham khảo
1	CVE-2023-28252	- Điểm: CVSS: 7.8 (cao) - Mô tả: lỗ hổng trong Windows Common Log File System Driver 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-2023-28252
2	CVE-2023-21554	- Điểm: CVSS: 9.8 (nghiêm trọng) - Mô tả: lỗ hổng trong Microsoft Message Queuing 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-2023-21554
3	CVE-2023-23384 CVE-2023-23375 CVE-2023-28304	- Điểm: CVSS: 7.8/7.3 (cao) - Mô tả: lỗ hổng trong Microsoft SQL Server cho phép đối tượng tấn công thực thi mã từ xa. - Ảnh hưởng: Microsoft SQL Server, Microsoft ODBC Driver 18.	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-23384 https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-23375 https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-28304
4	CVE-2013-3900	- Điểm: CVSS: 7.4 (cao) - Mô tả: lỗ hổng xác thực chữ ký WinVerifyTrust cho phép đối tượng tấn công có thể thêm nội dung	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2013-3900

		vào phần chữ ký mã xác thực trong tệp thực thi đã ký mà không làm mất hiệu lực chữ ký. - Ảnh hưởng: Windows Server, Windows 10/11.	
5	CVE-2023-28287 CVE-2023-28295	- Điểm: CVSS: 8.8 (cao) - Mô tả: lỗ hổng trong Microsoft Publisher cho phép đối tượng tấn công thực thi mã từ xa. - Ảnh hưởng: Microsoft Office, Microsoft Publisher.	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-28287 https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-28295
6	CVE-2023-28309 CVE-2023-28314	- Điểm: CVSS: 7.6/6.1 (cao) - Mô tả: lỗ hổng trong Microsoft Dynamics 365 cho phép đối tượng tấn công thực hiện tấn công XSS. - Ảnh hưởng: Microsoft Dynamics 365.	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-28309 https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-28314

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/2023/4/11/the-april-2023-security-update-review