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: /CATTT-NCSC
V/v lỗ hổng an toàn thông tin ảnh hưởng cao và nghiêm trọng trong các sản phẩm của Microsoft công bố tháng 06/2023

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 13/06/2023, Microsoft đã phát hành danh sách bản vá tháng 06 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 và nghiêm trọng sau:

- 02 lỗ hổng bảo mật **CVE-2023-32031, CVE-2023-28310** trong Microsoft Exchange Server cho phép đối tượng tấn công thực thi mã từ xa.

- 02 lỗ hổng bảo mật **CVE-2023-29357, CVE-2023-33142** trong Microsoft SharePoint Server cho phép đối tượng tấn công thực hiện nâng cao đặc quyền.

Trong thời gian vừa qua, Trung tâm Giám sát an toàn không gian mạng quốc gia (NCSC), Cục An toàn thông tin đã cảnh báo rộng rãi về các lỗ hổng ảnh hưởng đến Microsoft Exchange Server, Microsoft SharePoint Server tại văn bản số 158/CATTT-NCSC phát hành ngày 15/2/2023 và văn bản số 729/CATTT-NCSC phát hành ngày 15/05/2023. Qua đó cho thấy, Microsoft Exchange Server và Microsoft SharePoint Server vẫn luôn 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 nhằm thực hiện những hành động trái phép. Chính vì vậy, các cơ quan, tổ chức cần đặc biệt quan tâm cũng như có phương án khắc phục, xử lý kịp thời nếu bị ảnh hưởng và thực hiện tăng cường giám sát nhằm giảm thiểu nguy cơ bị tấn công thông qua các lỗ hổng này.

- 03 lỗ hổng bảo mật **CVE-2023-29363, CVE-2023-32014, CVE-2023-32015** trong Windows Pragmatic General Multicast (PGM) cho phép đối tượng tấn công thực thi mã từ xa.

- Lỗ hổng bảo mật **CVE-2023-3079** liên quan đến lỗi Type confusion 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 được khai thác trong thực tế.

- 03 lỗ hổng bảo mật **CVE-2023-32029, CVE-2023-33133, CVE-2023-33137** trong Microsoft Excel cho phép đối tượng tấn công thực thi mã từ xa.

- Lỗ hổng bảo mật **CVE-2023-33146** trong Microsoft Office cho phép đối tượng tấn công thực thi mã từ xa.

Thông tin chi tiết các lỗ hổng xin xem tại phụ lục gửi 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;
- Các Cục: Viễn thông, Bưu điện Trung ương;
- Các Trung tâm: TTTT, VNNIC;
- Cục trưởng (để b/c);
- Các Phó Cục trưởng;
- ATHTTT, VNCERT/CC;
- Lưu: VT, NCSC.

KT. CỤC TRƯỞNG
PHÓ CỤC TRƯỞNG

Trần Đăng Khoa

Phụ lục
THÔNG TIN VỀ CÁC LỖ HỔNG AN TOÀN THÔNG TIN TRONG SẢN PHẨM CỦA MICROSOFT
(Kèm theo Công văn số /CATTT-NCSC ngày / /2023 của Cục An toàn thông tin)

1. Thông tin các lỗ hổng an toàn thông tin

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.	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-3079

STT	CVE	Mô tả	Link tham khảo
		- Ảnh hưởng: Microsoft Edge (Chromium-based)	
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 an toàn thông tin 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