UBND TỈNH TÂY NINH
SỞ THÔNG TIN VÀ TRUYỀN THÔNG

Số: 1080 /STTTT-TTGSĐH
V/v cảnh báo lỗ hổng bảo mật có mức ảnh hưởng Cao trong các sản phẩm Microsoft công bố tháng 6/2023

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

Tây Ninh, ngày 06 tháng 7 năm 2023

Kính gửi:

- Văn phòng Tỉnh ủy;
- Văn phòng Đoàn ĐBQH và HĐND tỉnh;
- Văn phòng UBND tỉnh;
- Các cơ quan tham mưu, giúp việc Tỉnh ủy;
- Mặt trận Tổ quốc và các Đoàn thể chính trị - xã hội;
- Các Sở, ban, ngành tỉnh;
- Các huyện, thị, thành ủy trực thuộc Tỉnh ủy;
- UBND các huyện, thị xã, thành phố;
- UBND các xã, phường, thị trấn.

Thực hiện Công văn số 1024/CATTT-NCSC của Cục An toàn thông tin - Bộ Thông tin và Truyền thông về việc cảnh báo lỗ hổng bảo mật ảnh hưởng cao và nghiêm trọng trong các sản phẩm Microsoft công bố tháng 6/2023 ***(Thông tin chi tiết phụ lục kèm theo)***.

Nhằm đảm bảo an toàn thông tin cho hệ thống thông tin cho người dùng, đơn vị và toàn bộ hệ thống của tỉnh, Sở Thông tin và Truyền thông đề nghị các đơn vị, địa phương thực hiện gấp các công việc cụ thể như sau:

1. Kiểm tra, rà soát, xác định máy tính sử dụng hệ điều hành Windows và phần mềm có khả năng bị ảnh hưởng. Thực hiện cập nhật bản vá kịp thời theo hướng dẫn tại phụ lục để tránh nguy cơ bị tấn công.

2. Tăng cường kiểm tra, giám sát hệ thống mạng của đơn vị, địa phương, khi có phát hiện hoạt động tấn công mạng, đề nghị liên hệ Sở Thông tin và Truyền thông để phối hợp xử lý kịp thời.

Thông tin liên quan đề nghị liên hệ Ông Vương Duy Thanh - Trung tâm Giám sát, điều hành kinh tế, xã hội tập trung; Điện thoại: 0932624462.

Trân trọng./.

Nơi nhận:
- Như trên;
- GĐ Sở (b/c);
- P.CNTTBCVT;
- Lưu: VT, TTGSĐH.

KT. GIÁM ĐỐC
PHÓ GIÁM ĐỐC

CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM
SỞ THÔNG TIN VÀ TRUYỀN THÔNG
TỈNH TÂY NINH

Nguyễn Trung Hiếu

PHỤ LỤC
Thông tin các lỗ hổng nghiêm trọng trong các sản phẩm Microsoft công bố tháng 6/2023

1.Thông tin lỗ hổng bảo mật

- Mô tả:

- 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.

- Ảnh hưởng:

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	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-32031

STT	CVE	Mô tả	Link tham khảo
		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-2023-28310
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	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-32029

STT	CVE	Mô tả	Link tham khảo
		đối tượng tấn công thực thi mã từ xa. - Ảnh hưởng: Microsoft Excel, Microsoft Office.	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

- Đánh giá mức độ: Đánh giá sơ bộ từ các chuyên gia bảo mật, lỗ hổng này ảnh hưởng đến nhiều thiết bị trên toàn cầu trong đó có cả Việt Nam. Trung tâm Giám sát an toàn không gian mạng quốc gia (NCSC) đánh giá khả năng các mã khai thác của các lỗ hổng này sẽ sớm được công khai trên Internet trong thời gian sắp tới.

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. Nguồn tham khảo:

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

https://www.zerodayinitiative.com/blog/2023/6/13/the-june-2023-security-update-review