Cơ quan: THÀNH ỦY CẨM PHẢ
Email: tucp@quangninh.gov.vn
Thời gian ký: 29.08.2023 16:19:09 +07:00

ĐẢNG BỘ TỈNH QUẢNG NINH
THÀNH ỦY CẨM PHẢ
*
Số 1421 -CV/TU
V/v cảnh báo lỗ hổng bảo mật ảnh hưởng cao và nghiêm trọng trong các sản phẩm Microsoft công bố tháng 8/2023

ĐẢNG CỘNG SẢN VIỆT NAM

Cẩm Phả, ngày 29 tháng 8 năm 2023

Kính gửi: - Thường trực HĐND, Lãnh đạo UBND Thành phố,
- Các Ban xây dựng Đảng, Văn phòng Thành ủy,
- MTTQ và các tổ chức chính trị - xã hội Thành phố,
- Các chi, đảng bộ trực thuộc Thành ủy.

Căn cứ Văn bản số 2033/STTTT-CNTT ngày 25/8/2023 của Sở Thông tin và Truyền thông tỉnh về việc cảnh báo lỗ hổng bảo mật ảnh hưởng cao và nghiêm trọng trong các sản phẩm Microsoft công bố tháng 8/2023;

Nhằm bảo đảm an toàn thông tin và phòng tránh việc đối tượng tấn công lợi dụng điểm yếu an toàn thông tin để thực hiện những cuộc tấn công mạng nguy hiểm. Thường trực Thành ủy yêu cầu Thường trực HĐND, UBND Thành phố; các Ban xây dựng Đảng, Văn phòng Thành ủy; MTTQ và các tổ chức chính trị - xã hội Thành phố; các chi, đảng bộ trực thuộc Thành ủy khẩn trương chỉ đạo thực hiện ngay một số nội dung 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 (*Thông tin về lỗ hổng và cách khắc phục chi tiết 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.

Trong trường hợp cần thiết, yêu cầu Thủ trưởng các cơ quan, đơn vị và cá nhân liên quan khẩn trương liên hệ với đơn vị chức năng để được hỗ trợ, hướng dẫn xử lý:

- Trung tâm Công nghệ thông tin và Truyền thông, Sở Thông tin và Truyền thông, điện thoại: 0203 3533338, email: qnict@quangninh.gov.vn.

- Trung tâm Giám sát an toàn không gian mạng quốc gia thuộc Cục An toàn thông tin, điện thoại: 024.3209.1616, email: ais@mic.gov.vn.

Thừa lệnh Ban Thường vụ Thành ủy, Văn phòng Thành ủy thông báo ý kiến chỉ đạo của Thường trực Thành ủy để Thủ trưởng các cơ quan, đơn vị biết, chỉ đạo tổ chức thực hiện./.

Nơi nhận:
- Sở TTTT (*để báo cáo*),
- Thường trực Thành ủy (*để báo cáo*),
- Như kính gửi,
- Lưu VPTU.

T/L BAN THƯỜNG VỤ
CHÁNH VĂN PHÒNG

ĐẢNG CỘNG SẢN VIỆT NAM
THÀNH ỦY CẨM PHẢ
ĐẢNG BỘ TỈNH QUẢNG NINH

Vũ Hồng Chương

PHỤ LỤC

Thông tin về các lỗ hổng bảo mật trong sản phẩm Microsoft công bố tháng 6/2023 và hướng dẫn khắc phục

---

1. Thông tin các lỗ hổng bảo mật

STT	CVE	Mô tả	Link tham khảo
1	CVE-2023-38181	- Điểm: CVSS: 8.8 (Cao) - Mô tả: lỗ hổng trong Microsoft Exchange Server cho phép đối tượng tấn công thực hiện tấn công Spoofing. - Ảnh hưởng: Exchange Server 2016/2019.	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-38181
2	CVE-2023-21709	- Điểm: CVSS: 9.8 (được Microsoft đánh giá là Cao) - Mô tả: lỗ hổng trong Microsoft Exchange Server cho phép đối tượng tấn công thực hiện tấn công nâng cao đặc quyền. - Ảnh hưởng: Exchange Server 2016/2019.	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-21709
3	CVE-2023-35368 CVE-2023-38185 CVE-2023-35388 CVE-2023-38182	- Điểm: CVSS: 8.0/8.8 (Cao) - Mô tả: lỗ hổng trong Microsoft Exchange Server cho phép đối tượng tấn công thực thi mã từ xa. - Ảnh hưởng: Exchange Server 2016/2019.	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-35368 https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-38185 https://msrc.microsoft.com/update-

			guide/vulnerability/CVE-2023-35388 https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-38182
4	CVE-2023-35385 CVE-2023-36910 CVE-2023-36911	- 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 10/11, Windows Server.	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-35385 https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-36910 https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-36911
5	CVE-2023-29328 CVE-2023-29330	- Điểm: CVSS: 8.8 (được Microsoft đánh giá là Nghiêm trọng) - Mô tả: lỗ hổng trong Microsoft Teams cho phép đối tượng tấn công thực thi mã từ xa. - Ảnh hưởng: Microsoft Teams dành cho iOS, Mac, Android, Desktop	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-29328 https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-29330
6	CVE-2023-36895	- Điểm: CVSS: 7.8 (được Microsoft đánh giá là Nghiêm trọng) - Mô tả: lỗ hổng trong Microsoft Outlook cho phép đối tượng tấn công thực thi mã từ xa.	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-36895

		- Ảnh hưởng: Microsoft Office, Microsoft 365 Apps for Enterprise.	
7	CVE-2023-36896	- 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, Office, Office LTSC, 365 Apps.	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-36896
8	CVE-2023-35371	- 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, Office LTSC, 365 Apps.	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-35371

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. Các cơ quan, 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/2023/8/8/the-august-2023-security-update-review