UBND TỈNH TUYÊN QUANG
SỞ THÔNG TIN VÀ TRUYỀN THÔNG

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

Số: 1121 /STTTT-CNTT&BCVT
V/v lỗ hổng bảo mật ảnh hưởng mức Cao và Nghiêm trọng trong các sản phẩm Microsoft công bố tháng 9/2022

Tuyên Quang, ngày 29 tháng 9 năm 2022

Kính gửi:
- Văn phòng Đoàn Đại biểu Quốc hội và Hội đồng nhân dân;
- Văn phòng Ủy ban nhân dân tỉnh;
- Các sở, ban, ngành;
- Các tổ chức-Chính trị xã hội;
- Uỷ ban nhân dân các huyện, thành phố.

Căn cứ văn bản số1442/CATTT –NCSC ngày 23/9/2022 của Cục An toàn thông tin về việc lỗ hổng bảo mật ảnh hưởng Cao và Nghiêm trọng trong các sản phẩm Microsoft công bố tháng 9/2022, Sở Thông tin và Truyền thông cung cấp thông tin và đưa ra các giải pháp phòng, tránh khai thác lỗ hổng bảo mật trong các sản phẩm Microft như sau:

I.Thông tin về lỗ hổng bảo mật trong các sản phẩm Microsoft

Ngày 13/9/2022, Microsoft đã phát hành danh sách bản vá tháng 9 với 64 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-2022-37969** trong Windows Common Log File System Driver cho phép đối tượng tấn công thực hiện nâng cao đặc quyền. Lỗ hổng này đang được khai thác rộng rãi trên Internet.
- Lỗ hổng bảo mật **CVE-2022-34718** trong Windows TCP/IP cho phép đối tượng tấn công chưa xác thực có thể thực thi mã từ xa.
- Lỗ hổng bảo mật **CVE-2022-34724** trong Windows DNS Server cho phép đối tượng tấn công thực hiện tấn công từ chối dịch vụ.
- Lỗ hổng bảo mật **CVE-2022-3075** trong Chromium cho phép đối tượng tấn công chưa xác thực có thể thực thi mã từ xa.
- 02 lỗ hổng bảo mật **CVE-2022-34721, CVE-2022-34722** trong Windows Internet Key Exchange (IKE) Protocal Extensions cho phép đối tượng tấn công thực thi mã từ xa. Mã khai thác của các lỗ hổng này đã được công bố rộng rãi trên Internet.
- 04 lỗ hổng bảo mật **CVE-2022-37961, CVE-2022-35823, CVE-2022-38008, CVE-2022-38009** trong Microsoft SharePoint Server cho phép đối tượng tấn công

thực thi mã từ xa.

- Lỗ hổng bảo mật **CVE-2022-37962** trong Microsoft PowerPoint cho phép đối tượng tấn công thực thi mã từ xa khi người dùng mở tập tin PowerPoint độc hại..

(Thông tin chi tiết các lỗ hổng bảo mật có tại phụ lục kèm theo).

II. Các giải pháp phòng tránh

Nhằm đảm bảo an toàn thông tin cho hệthống thông tin của Quý cơ quan đơn vị, góp phần bảo đảm an toàn cho không gian mạng Việt Nam, SởThông tin và Truyền thông đề nghịcác sở, ban, ngành, Ủy ban nhân dân các huyện, thành phốtriển khai 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;
- Ban Giám đốc sở (báo cáo);
- Các đơn vị thuộc sở;
- Lưu VT, CNTT&BCVT.

KT.GIÁM ĐỐC
PHÓ GIÁM ĐỐC

CỘNG HOÀ X.H.C.N VIỆT NAM
SỞ THÔNG TIN VÀ TRUYỀN THÔNG
TỈNH TUYÊN QUANG

Nguyễn Văn Hiến

Phụ lục
THÔNG TIN VỀ CÁC LỖ HỔNG BẢO MẬT
TRONG SẢN PHẨM MICROSOFT
(Kèm theo Công văn số 1121 /STTTT-CNTT&BCVT ngày 29 / 9 /2022 của Sở Thông tin và Truyền thông)

1. Thông tin các lỗ hổng bảo mật

STT	CVE	Mô tả	Link tham khảo
1	CVE-2022-37969	- Điểm CVSS: 7.8 (Cao) - Lỗ hổng trong Windows Common Log File System Driver cho phép đối tượng tấn công thực thi mã từ xa với các đặc quyền nâng cao. - Ảnh hưởng: Windows 7/8.1/10/11, Windows Server 2008/2012/2016/2019/2022.	https://msrc.microsoft.coc/update-guide/vulnerability/CVE-2022-37969
2	CVE-2022-34718	- Điểm CVSS: 9.8 (Nghiêm trọng) - Lỗ hổng trong Windows TCP/IP cho phép đối tượng tấn công chưa xác thực có thể thực thi mã từ xa. - Ảnh hưởng: Windows 7/8.1/10/11,Windows Server 2008/2012/2016/2019/2022.	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-34718
3	CVE-2022-34724	- Điểm CVSS: 7.5 (Cao) - Lỗ hổng trong Windows DNS Server cho phép đối tượng tấn công thực hiện tấn công từ chối dịch vụ. - Ảnh hưởng: Windows Server 2008/2012/2016/2019/2022.	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-34724
4	CVE-2022-3075	- Lỗ hổng trong Chromium cho phép đối tượng tấn công chưa xác thực có thể thực thi mã từ xa. - Ảnh hưởng: Microsoft Egde (Chromium-based)	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-3075
5	CVE-2022-34721, CVE-2022-34722	- Điểm CVSS: 9.8 (Nghiêm trọng) - Lỗ hổng trong Windows Internet Key Exchange (IKE) Protocal Extensions cho phép	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-34721 https://msrc.microsoft

		đối tượng tấn công thực thi mã từ xa. - Ảnh hưởng: Windows 7/8.1/10/11, Windows Server 2008/2012/2016/2019/2022.	.com/update-guide/vulnerability/CVE-2022-34722
6	CVE-2022-37961 CVE-2022-35823 CVE-2022-38008 CVE-2022-38009	- Điểm CVSS: 7.8 (Cao) - Lỗ hổng trong Microsoft SharePoint Server cho phép đối tượng tấn công thực thi mã từ xa. - Ảnh hưởng: Microsoft SherePoint Foundation 2013, SharePoint Server 2013/2016/2019, Microsoft SharePoint Enterprise Server 2013.	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-37961 https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-35823 https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-38008 https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-38009
7	CVE-2022-37962	- Điểm CVSS: 7.8 (Cao) - Lỗ hổng trong Microsoft PowerPoint cho phép đối tượng tấn công thực thi mã từ xa. - Ảnh hưởng: Microsoft Office 2013/2016/2019, Office 365 Apps, Office LTSC 2021.	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-37962

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/releaseNote/2022-Sep

https://www.zerodayinitiative.com/blog/2022/9/13/the-september-2022-security-update-review