UBND TỈNH QUẢNG NGÃI **SỞ THÔNG TIN VÀ TRUYỀN THÔNG**	**CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM** **Độc lập - Tự do - Hạnh phúc**
Số:1374 /STTTT-BCVT&CNTT	*Quảng Ngãi, ngày 27 tháng 9 năm 2022*

V/v cảnh báo lỗ hổng bảo mật ảnh hưởng cao trong các sản phẩm Microsoft công bố tháng 9/2022

Kính gửi:

- Văn phòng: Tỉnh ủy, Đoàn ĐBQH&HĐND, UBND tỉnh;
- Các sở, ban, ngành; Hội, đoàn thể tỉnh;
- UBND các huyện, thị xã, thành phố;
- Báo Quảng Ngãi, Đài Phát thanh và Truyền hình tỉnh;
- Phòng An ninh mạng và phòng, chống tội phạm sử dụng công nghệ cao - Công an tỉnh;
- UBND các xã, phường, thị trấn.

Theo cảnh báo của Cục An toàn thông tin tại Công văn số 1442/CATTT-NCSC ngày 23/9/2022 về 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 đề nghị lãnh đạo các cơ quan, đơn vị chỉ đạo thực hiện một số biện pháp sau để hạn chế các rủi ro về nguy cơ mất an toàn thông tin:

1. Kiểm tra, rà soát máy chủ, máy trạm có sử dụng hệ điều hành Windows để phát hiện và xử lý kịp thời các máy chủ có khả năng bị ảnh hưởng bởi các lỗ hổng bảo mật 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. *(tham khảo thông tin lỗ hổng và cách khắc phục tại Phụ lục Thông tin về lỗ hổng bảo mật kèm theo Công văn này)*.

2. Khi phát hiện các hệ thống có biểu hiện bị khai thác, tấn công mạng, triển khai ngay các biện pháp xử lý ngăn chặn tấn công trên hệ thống và thông báo về Đội ứng cứu sự cố an toàn thông tin mạng tỉnh Quảng Ngãi để có các biện pháp hỗ trợ, xử lý kịp thời.

Đề nghị lãnh đạo các cơ quan, đơn vị quan tâm chỉ đạo thực hiện./.

***Nơi nhận*:**
- Như trên;
- Phòng VH&TT các huyện, thị xã, thành phố;
- Thành viên Đội ứng cứu sự cố ATTT mạng tỉnh;
- Sở TT&TT: Lãnh đạo Sở,
  các phòng chuyên môn, TT CN TT&TT;
- Lưu: VT, BCVT&CNTT.

KT. GIÁM ĐỐC
PHÓ GIÁM ĐỐC

CỘNG HÒA X.H.C.N VIỆT NAM
SỞ THÔNG TIN VÀ TRUYỀN THÔNG
TỈNH QUẢNG NGÃI

Đỗ Quang Nghĩa

PHỤ LỤC
THÔNG TIN VỀ CÁC LỖ HỔNG BẢO MẬT TRONG MICROSOFT

(Kèm theo Công văn số /STTTT-BCVT&CNTT ngày /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.com/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	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-3075

STT	CVE	Mô tả	Link tham khảo
		xa. - Ảnh hưởng: Microsoft Egde (Chromium-based)	
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 đối tượng tấn công 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-2022-34721 https://msrc.microsoft.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