UBND HUYỆN BÌNH SƠN
PHÒNG VĂN HÓA VÀ THÔNG TIN

Số: 215 /VHTT-CNTT

V/v cảnh báo lỗ hổng bảo mật ảnh hưởng cao trong các sản phẩm Microsoft công bố tháng 8/2022

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

Bình Sơn, ngày 15 tháng 8 năm 2022

Kính gửi:
- Các phòng, ban, ngành thuộc huyện;
- UBND các xã, thị trấn.

Thực hiện Công văn số 1138/STTTT-BCVT&CNTT ngày 15/8/2022 của Sở Thông tin và Truyền thông về việc cảnh báo lỗ hổng bảo mật ảnh hưởng cao trong các sản phẩm Microsoft công bố tháng 8/2022 và cảnh báo của Cục An toàn thông tin tại Công văn số 1221/CATTT-NCSC ngày 10/8/2022 về lỗ hổng bảo mật ảnh hưởng Cao và Nghiêm trọng trong các sản phẩm Microsoft công bố tháng 8/2022; Phòng Văn hóa và Thông tin huyện 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-2022-34713** trong Microsoft Windows Support Diagnostic Tool(MSDT) cho phép đối tượng tấn công thực thi mã từ xa. Lỗ hổng này đang được khai thác rộng rãi trên Internet.

- 04 lỗ hổng bảo mật **CVE-2022-21980, CVE-2022-24477, CVE-2022-24516**, **CVE-2022-30134** trong Microsoft Exchange Server cho phép đối tượng tấn công thu thập thông tin và thực hiện leo thang đặc quyền.

- Lỗ hổng bảo mật **CVE-2022-35804** trong SMB Client and Server cho phép đối tượng tấn công thực thi mã từ xa trên phiên bản Windows 11.

- Lỗ hổng bảo mật **CVE-2022-34715** trong Windows Network File System cho phép đối tượng tấn công chưa xác thực có thể thực thi mã từ xa.

- Lỗ hổng bảo mật **CVE-2022-35742** trong Microsoft Outlook cho phép đối tượng tấn công thực hiện tấn công từ chối dịch vụ *(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;
- UBND huyện (báo cáo);
- PVHTT: TP, PTP, CVIT;
- Lưu: VT.

KT. TRƯỞNG PHÒNG
PHÓ TRƯỞNG PHÒNG

CỘNG HÒA X.H.C.N VIỆT NAM
PHÒNG VĂN HÓA VÀ THÔNG TIN
H. BÌNH SƠN - T. QUẢNG NGÃI

Nguyễn Chung

PHỤ LỤC

THÔNG TIN VỀ CÁC LỖ HỔNG BẢO MẬT TRONG MICROSOFT

(Kèm theo Công văn số 215/VHTT-CNTT ngày 15/8/2022 của Phòng Văn hóa và Thông tin)

1. Thông tin các lỗ hổng bảo mật

STT	CVE	Mô tả	Link tham khảo
1	CVE-2022-34713	- Điểm CVSS: 7.8 (Cao) - Lỗ hổng trong Microsoft Windows Support Diagnostic Tool (MSDT) cho phép đối tượng tấn công thực thi mã từ xa. - Ảnh hưởng: Windows 7/8.1/10/11, Windows Server 2008/2012.	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-34713
2	CVE-2022-21980 CVE-2022-24477 CVE-2022-24516 CVE-2022-30134	- Điểm CVSS: 8.0 (Cao) - Lỗ hổng trong Microsoft Exchange Server cho phép đối tượng tấn công thu thập thông tin và thực hiện leo thang đặc quyền. - Ảnh hưởng: Microsoft Exchange Server 2013/2016/2019.	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-21980 https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-24477 https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-24516 https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-30134
3	CVE-2022-35804	- Điểm CVSS: 8.8 (Cao) - Lỗ hổng trong SMB Client and Server cho phép đối tượng tấn công chưa xác thực có thể thực thi mã từ xa. - Ảnh hưởng: Windows 11.	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-35804

STT	CVE	Mô tả	Link tham khảo
4	CVE-2022-34715	- Điểm CVSS: 9.8 (Nghiêm trọng) - Lỗ hổng trong Windows Network File System cho phép đối tượng tấn công chưa xác thực có thể thực thi mã từ xa. - Ảnh hưởng: Windows Server 2022.	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-34715
5	CVE-2022-35742	- Điểm CVSS: 7.5 (Cao) - Lỗ hổng trong Microsoft Outlook cho phép đối tượng tấn công thực hiện tấn công từ chối dịch vụ. - Ảnh hưởng: Microsoft Outlook 2012/2016, Microsoft Office LTSC 2021/2019, Microsoft 365 Apps.	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-35742

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-Aug

https://www.zerodayinitiative.com/blog/2022/8/9/the-august-2022-security-update-review