UBND TỈNH BÌNH ĐỊNH
SỞ THÔNG TIN VÀ TRUYỀN THÔNG

Số: 115 /STTTT-BCVT&CNTT

V/v cảnh báo lỗ hổng bảo mật ảnh hưởng cao và nghiêm trọng trong các sản phẩm Microsoft công bố tháng 02/2022

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

Bình Định, ngày 10 tháng 02 năm 2022

Kính gửi:
- Các sở, ban, ngành;
- UBND các huyện, thị xã, thành phố.

Thực hiện khuyến nghị của Cục An toàn thông tin thuộc Bộ Thông tin và Truyền thông tại Công văn số 163/CATTT-NCSC ngày 09/02/2022 về lỗ hổng bảo mật ảnh hưởng cao và nghiêm trọng trong các sản phẩm Microsoft công bố tháng 02/2022;

Nhằm đảm bảo an toàn thông tin cho hệ thống thông tin của Quý cơ quan, đơn vị, góp phần bảo đảm an toàn cho các hoạt động trên môi trường mạng, Sở Thông tin và Truyền thông đề nghị các cơ quan, đơn vị thực hiện các nội dung:

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 (*có hướng dẫn chi tiết tại Phụ lục kèm theo*).

2. Tăng cường giám sát hệ thống mạng tại cơ quan đơn vị, kịp thời phát hiện hoạt động tấn công mạng; phối hợp với Đội ứng cứu sự cố an toàn thông tin mạng của tỉnh trong xử lý, ứng cứu sự cố gây mất an toàn thông tin khi tham gia hoạt động trên môi trường mạng tại cơ quan, đơn vị.

Trong quá trình triển khai nếu cần hỗ trợ liên hệ: Phòng Bưu chính, Viễn thông và Công nghệ thông tin, điện thoại: 0256.2210517.

Đề nghị Quý cơ quan, đơn vị quan tâm phối hợp, thực hiện./.

Nơi nhận:
- Như trên;
- Giám đốc Sở (để b/cáo);
- Công an tỉnh - PA 03 (để p/hợp);
- TT.CNTT&TT (để t/hiện);
- 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 BÌNH ĐỊNH

Nguyễn Minh Thảo

PHỤ LỤC

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

(Kèm theo Công văn số /STTTT-BCVT&CNTT ngày /02/2022 của Sở Thông tin và Truyền thông)

1. Thông tin các lỗ hổng bảo mật

STT	CVE	Mô tả	Link tham khảo
1	CVE-2022-22005	- Điểm CVSS: 8.8 (cao) - Lỗ hổng trong Microsoft SharePoint Server, cho phép đối tượng tấn công thực thi mã từ xa. - Ảnh hưởng: Microsoft SharePoint Server 2019, SharePoint Enterprise Server 2013/2016.	https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2022-22005
2	CVE-2022-21989	- Điểm CVSS: 7.8 (cao) - Lỗ hổng trong Microsoft Kernel, cho phép đối tượng tấn công thực hiện tấn công nâng cao đặc quyền. - Ảnh hưởng: Windows Server 2022/2019/2016/2012/2008, Windows 11/10/8.1/7.	https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2022-21989
3	CVE-2022-21984	- Điểm CVSS: 8.8 (cao) - Lỗ hổng trong Windows DNS Server, cho phép đối tượng tấn công thực thi mã từ xa. - Ảnh hưởng: Windows 10/11, Windows Server 2022.	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-21984
4	CVE-2022-21995	- Điểm CVSS: 7.9 (cao) - Lỗ hổng trong Windows Hyper-V, cho phép đối tượng tấn công thực thi mã từ xa. - Ảnh hưởng: Windows 10/11, Windows Server 2022/2019/2016.	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-21995

5	CVE-2022-22718	- Điểm CVSS: 7.8 (cao) - Lỗ hổng trong Windows Print Sooler, cho phép đối tượng tấn công thực hiện tấn công nâng cao đặc quyền. - Ảnh hưởng: Windows Server 2022/2016/2012/2008, Windows 11/10/8.1/7.	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-22718
6	CVE-2022-22000	- Điểm CVSS: 7.8 (cao) - Lỗ hổng trong Windows Common Log File System Driver, cho phép đối tượng tấn công thực hiện tấn công nâng cao đặc quyền, đã có mã khai thác thành công được sử dụng trong TianfuCup. - Ảnh hưởng: Windows Server 2022/2019/2016/2012/2008, Windows 11/10/8.1/7.	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-22000
7	CVE-2022-21999	- Điểm CVSS: 7.8 (cao) - Lỗ hổng trong Windows Print Sooler, cho phép đối tượng tấn công thực hiện tấn công nâng cao đặc quyền, đã có mã khai thác thành công được sử dụng trong TianfuCup. - Ảnh hưởng: Windows Server 2022/2016/2012/2008, Windows 11/10/8.1/7.	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-21999
8	CVE-2022-21981	- Điểm CVSS: 7.8 (cao) - Lỗ hổng trong Windows Common Log File System Driver, cho phép đối tượng tấn công thực hiện tấn công nâng cao đặc quyền, đã có mã	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-21981

		khai thác thành công được sử dụng trong TianfuCup. - Ảnh hưởng: Windows Server 2019/2012/2008, Windows 11/10/8.1/7.	
9	CVE-2022-21996	- Điểm CVSS: 7.8 (cao) - Lỗ hổng trong Windows32k, cho phép đối tượng tấn công thực hiện tấn công nâng cao đặc quyền, đã có mã khai thác thành công được sử dụng trong TianfuCup. - Ảnh hưởng: Windows 11.	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-21996
10	CVE-2022-22715	- Điểm CVSS: 7.8 (cao) - Lỗ hổng trong Named Pipe File System, cho phép đối tượng tấn công thực hiện tấn công nâng cao đặc quyền, đã có mã khai thác thành công được sử dụng trong TianfuCup. - Ảnh hưởng: Windows 11/10, Windows Server 2022.	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-22715

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/

https://www.zerodayinitiative.com/blog/2022/2/8/the-february-2022-security-update-review