UBND TỈNH HÀ NAM
SỞ THÔNG TIN VÀ TRUYỀN THÔNG

Số: 259 /STTTT-BCVTCNTT

V/v lỗ hổng bảo mật ảnh hưởng cao và nghiêm trọng trong các sản phẩm Microsoft công bố tháng 3/2022

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

Hà Nam, ngày 10 tháng 3 năm 2022

Kính gửi:

- Văn phòng Tỉnh ủy Hà Nam;
- Các sở, ban, ngành, cơ quan, đoàn thể của tỉnh;
- UBND các huyện, thị xã, thành phố.

Căn cứ Công văn số 315/CATTT-NCSC ngày 09/3/2022 của Cục An toàn thông tin, Bộ Thông tin và Truyền thông về lỗ hổng bảo mật ảnh hưởng cao và nghiêm trọng trong các sản phẩm Microsoft công bố tháng 3/2022;

Nhằm tăng cường công tác bảo đảm an toàn, an ninh thông tin, đặc biệt là bảo vệ các hệ thống thông tin của các cơ quan, đơn vị trên địa bàn tỉnh, Sở Thông tin và Truyền thông đề nghị các cơ quan, đơn vị:

- 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. *(Chi tiết tại phụ lục kèm theo).*

- 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.

Đầu mối liên hệ, hỗ trợ:

- Sở Thông tin và Truyền thông (Trung tâm Công nghệ thông tin và Truyền thông - Bộ phận thường trực Đội Ứng cứu sự cố an toàn thông tin mạng tỉnh Hà Nam). Điện thoại: **0226.3846333**. Email: **ttcntt@hanam.gov.vn**

- Trung tâm Giám sát an toàn thông tin mạng quốc gia (NCSC), Cục An toàn thông tin. Điện thoại di động: **0243.2091616**. Email: **ais@mic.gov.vn**./.

Nơi nhận:
- Như trên;
- Lưu VT.

KT. GIÁM ĐỐC
PHÓ GIÁM ĐỐC

CỘNG HÒA XHCN VIỆT NAM
SỞ THÔNG TIN VÀ TRUYỀN THÔNG
TỈNH HÀ NAM

Nguyễn Đức Cường

Phụ lục

THÔNG TIN VÀ HƯỚNG DẪN KHẮC PHỤC CÁC LỖ HỔNG BẢO MẬT

(Kèm theo Công văn số /STTTT-BCVTCNTT ngày /3/2022 của Sở Thông tin và Truyền thông Hà Nam)

1. Thông tin về các lỗ hổng

STT	CVE	Mô tả	Link tham khảo
1	CVE-2022-21990	- Điểm CVSS: 8.8 (Cao) - Lỗ hổng trong Remote Desktop Client cho phép đối tượng tấn công thực thi mã từ xa. - Ảnh hưởng: Windows Server 2008/2012/2016/2019/2022, Windows 11/10/8.1/7.	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-21990
2	CVE-2022-23285	- Điểm CVSS: 8.8 (Cao) - Lỗ hổng trong Remote Desktop Client cho phép đối tượng tấn công thực thi mã từ xa. - Ảnh hưởng: Windows Server 2008/2012/2016/2019/2022, Windows 10/8.1/7.	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-23285
3	CVE-2022-24459	- Điểm CVSS: 7.8 (Cao) - Lỗ hổng Windows Fax và Scan Service cho phép đối tượng tấn công thực hiện tấn công leo thang đặc quyền. - Ảnh hưởng: Windows Server 2008/2012/2016/2019/2022, Windows 11/10/8.1/7.	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-24459
4	CVE-2022-24508	- Điểm CVSS: 8.8 (Cao) - Lỗ hổng trong trong SMBv3 cho phép đối tượng tấn công thực thi mã từ xa trên Windows SMBv3 Client/Server. - Ảnh hưởng: Windows 10/11, Windows Server 2022.	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-24508
5	CVE-2022-23277	- Điểm CVSS: 8.8 (Cao) - Lỗ hổng trong Microsoft Exchange Server cho phép đối tượng tấn công thực thi mã từ xa với tài	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-23277

STT	CVE	Mô tả	Link tham khảo
		khoản xác thực hợp lệ. - Ảnh hưởng: Microsoft Exchange Server 2019/2016/2013.	
6	CVE-2022-21967	- Điểm CVSS: 7.0 (Cao) - Lỗ hổng trong trong Xbox Live Auth Manager for Windows cho phép đối tượng tấn công thực hiện tấn công leo thang đặc quyền. - Ảnh hưởng: Windows 10/11.	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-21967
7	CVE-2022-22006	- Điểm CVSS: 7.8 (Cao) - Lỗ hổng trong HEVC Video Extensions, cho phép đối tượng tấn công thực thi mã từ xa. - Ảnh hưởng: HEVC Video Extensions.	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-22006
8	CVE-2022-24501	- Điểm CVSS: 7.8 (Cao) - Lỗ hổng trong VP9 Video Extensions, cho phép đối tượng tấn công thực thi mã từ xa. - Ảnh hưởng: VP9 Video Extensions.	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-24501

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. 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. Nguồn tham khảo

https://msrc.microsoft.com/update-guide/releaseNote/2022-Mar
https://msrc.microsoft.com/update-guide/en-us