UBND TỈNH HÀ NAM
SỞ THÔNG TIN VÀ TRUYỀN THÔNG

Số: 419 /STTTT-BCVTCNTT

V/v lỗ hổng bảo mật ảnh hưởng cao và nghiêm trọng trong các sản phẩm Microsoft công bố tháng 4/2022

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

Hà Nam, ngày 20 tháng 4 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 508/CATTT-NCSC ngày 13/4/2022 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 4/2022;

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 / /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-2022-26809	- Điểm CVSS: 9.8 (Nghiêm trọng) - Lỗ hổng trong RPC Runtime Library cho phép đối tượng tấn công thực thi mã từ xa với đặc quyền cao trên hệ thống bị ảnh hưởng. - Ảnh hưởng: Windows 7/8.1/10/11, Windows Server 2008/2012/2016/2019/2022.	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-26809
2	CVE-2022-24491	- Điểm CVSS: 9.8 (Nghiêm trọng) - Lỗ hổng trong Windows Network File System cho phép đối tượng tấn công thực thi mã từ xa với đặc quyền cao. - Ảnh hưởng: Windows 8.1/10/11, Windows Server 2012/2016/2019.	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-24491
3	CVE-2022-24497	- Điểm CVSS: 9.8 (Nghiêm trọng) - Lỗ hổng trong Windows Network File System cho phép đối tượng tấn công thực thi mã từ xa. - Ảnh hưởng: Windows 8.1/10, Windows Server 2012/2016/2019/2022.	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-24497
4	CVE-2022-26815	- Điểm CVSS: 7.2 (cao) - Lỗ hổng trong Windows DNS Server cho phép đối tượng tấn công thực thi mã từ xa.	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-26815

STT	CVE	Mô tả	Link tham khảo
		- Ảnh hưởng: Windows Server 2008/2012/2016/2019/2022.	
5	CVE-2022-26904	- Điểm CVSS: 7.9 (cao) - Lỗ hổng trong Windows User Profile Service cho phép đối tượng tấn công thực hiện nâng cao đặc quyền. Lỗ hổng này đã có mã khai thác công khai trên Internet. - Ảnh hưởng: Windows 7/8.1/10/11, Windows Server 2008/2012/2016.	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-26904
6	CVE-2022-26919	- Điểm CVSS: 8.1 (Cao) - Lỗ hổng trong Windows LDAP cho phép đối tượng tấn công thực thi mã từ xa. - Ảnh hưởng: Windows 8.1/10/11, Windows Server 2008/2012/2016/2019/2022.	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-26919
7	CVE-2022-24521	- Điểm CVSS: 7.8 (Cao) - Lỗ hổng trong Windows Common Log File System Driver cho phép đối tượng tấn công thực hiện nâng cao đặc quyền. - Ảnh hưởng: Windows 7/8.1/10/11, Windows Server 2008/2012/2016/2019/2022.	https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2022-24521

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-Apr

https://www.zerodayinitiative.com/blog/2022/4/11/the-april-2022-security-update-review