UBND TỈNH NGHỆ AN
SỞ THÔNG TIN VÀ TRUYỀN THÔNG

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

Số: 723 /STT&TT-CNTT

V/v cảnh báo lỗ hổng bảo mật ảnh hưởng cao và nghiêm trọng trong các sản phẩm Microsoft công bố tháng 05/2022

Nghệ An, ngày 12 tháng 5 năm 2022

Kính gửi:
- Các Sở, ban, ngành cấp tỉnh;
- UBND các huyện, thành phố, thị xã;
- Các tổ chức Chính trị – Xã hội;
- Phòng cơ yếu, CNTT – Văn phòng Tỉnh uỷ.

Ngày 11/05/2022, Cục An toàn thông tin, Bộ Thông tin và Truyền thông đã có công văn số 674/CATTT-NCSC về lỗ hổng bảo mật ảnh hưởng cao và nghiêm trọng trong các sản phẩm Microsoft công bố tháng 05/2022. Theo văn bản này, Cục An toàn thông tin cung cấp thông tin:

Ngày 10/5/2022, Microsoft đã phát hành danh sách bản vá tháng 5 với 74 lỗ hổng bảo mật trong các sản phẩm của mình. Bản phát hành tháng này đặc biệt đáng chú ý các lỗ hổng bảo mật sau:

Các lỗ hổng bảo mật có mức ảnh hưởng Nghiêm trọng:

- Lỗ hổng bảo mật CVE-2022-26925 trong Windows LSA cho phép đối tượng tấn công không cần xác thực có thể thực hiện tấn công giả mạo (spoofing). Trong thực tế, lỗ hổng này đang được sử dụng kết hợp với NTLM relay attack, từ đó giúp đối tượng tấn công nâng cao đặc quyền trong hệ thống mục tiêu.

- Lỗ hổng bảo mật CVE-2022-26937 trong Windows Network File System cho phép đối tượng tấn công thực thi mã từ xa.

- Lỗ hổng bảo mật CVE-2022-29972 trong Magnitude Simba Amazon Redshift ODBC Driver cho phép đối tượng thực thi mã từ xa.

Các lỗ hổng bảo mật có mức ảnh hưởng Cao:

- Lỗ hổng bảo mật CVE-2022-26923 trong Active Directory Domain Services cho phép đối tượng tấn công thực hiện nâng cao đặc quyền.

- Lỗ hổng bảo mật CVE-2022-21978 trong Microsoft Exchange Server cho phép đối tượng tấn công thực hiện nâng cao đặc quyền.

- Lỗ hổng bảo mật CVE-2022-22017 trong Remote Desktop Protocol Client cho phép đối tượng tấn công thực thi mã từ xa.

- Lỗ hổng bảo mật CVE-2022-29110 trong Microsoft Excel cho phép đối tượng tấn công thực thi mã từ xa.

- Lỗ hổng bảo mật CVE-2022-29108 trong Microsoft SharePoint Server cho phép đối tượng tấn công thực thi mã từ xa.

(Thông tin chi tiết các lỗ hổng bảo mật có tại phụ lục kèm theo).

Nhằm đảm bảo an toàn thông tin cho hệ thống thông tin của các cơ quan nhà nước cuả tỉnh, Sở Thông tin và Truyền thông đề nghị Lãnh đạo các đơn vị chỉ đạo các đơn vị, cá nhân có liên quan thuộc phạm vi quản lý thực hiện một số khuyến nghị của Bộ Thông tin và Truyền thông như sau:

1. Các giải pháp kỹ thuật khuyến nghị

- 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 (*tham khảo thông tin 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..

2. Đề nghị Phòng cơ yếu, CNTT – Văn phòng Tỉnh uỷ tham mưu văn bản thông báo cho các tổ chức cơ sở Đảng để biết và thực hiện.

3. Đề nghị Cổng Thông tin điện tử Nghệ An

- Đăng tải toàn văn nội dung công văn 674/CATTT-NCSC của Cục An toàn thông tin, Bộ Thông tin và Truyền thông lên Cổng thông tin điện tử tỉnh Nghệ An.

- Tổ chức kiểm tra, rà soát, kịp thời có phương án xử lý đối với các hệ thống hiện đang chủ trì quản trị kỹ thuật.

- Bố trí cán bộ kỹ thuật thường xuyên theo dõi hệ thống, hỗ trợ người sử dụng khi có nhu cầu.

4. Giao Trung tâm CNTT&TT Nghệ An

- Tổ chức kiểm tra, rà soát, kịp thời có phương án xử lý đối với các hệ thống hiện đang chủ trì quản trị kỹ thuật, đặc biệt hệ thống mạng máy tính của Sở Thông tin và Truyền thông.

- Bố trí đủ cán bộ thuộc bộ phận ứng cứu sự cố sẵn sàng thực hiện nhiệm vụ khi có điều động.

- Nghiên cứu giải pháp hỗ trợ các đơn vị khắc phục sự cố khi có yêu cầu.

5. Viễn thông Nghệ An (nhà cung cấp dịch vụ hệ thống VNPT-IOffice và VNPT-IGate)

Tuân thủ các quy định pháp lý hiện hành và các điều khoản thuộc hợp đồng thuê dịch vụ có liên quan đến công tác an toàn thông tin để đảm bảo hoạt động ổn định, an toàn các hệ thống: Cổng dịch vụ công trực tuyến tỉnh Nghệ An;

Hệ thống phần mềm quản lý văn bản VNPT IOffice.

Mọi thông tin cần hỗ trợ đề nghị Quý cơ quan, tổ chức, cá nhân liên hệ: Trung tâm Giám sát an toàn không gian mạng quốc gia (NCSC), điện thoại 02432091616, thư điện tử: ais@mic.gov.vn./.

Nơi nhận:
- Như trên;
- Cục ATTT, Bộ TT&TT (b/c);
- UBND tỉnh Nghệ An (b/c);
- VNPT Nghệ An;
- Ban Giám đốc Sở;
- Cổng TTĐT Nghệ An;
- TrT. CNTT&TT Nghệ An;
- Lưu: VT, CNTT.

KT. GIÁM ĐỐC
PHÓ GIÁM ĐỐC

Phan Nguyên Hào

Phụ lục Thông tin lỗ hổng bảo mật

(Kèm theo Công văn số /STT&TT-CNTT ngày 12/05/2022 của Sở Thông tin và Truyền thông tỉnh Nghệ An)

1. Thông tin các lỗ hổng bảo mật

STT	CVE	Mô tả	Link tham khảo
1	CVE-2022-26925	- Điểm CVSS: 9.8 (Nghiêm trọng) - Lỗ hổng trong Windows LSA cho phép đối tượng tấn công không cần xác thực có thể thực hiện tấn công giả mạo (spoofing) kết hợp với NTLM relay attack từ đó nâng cao đặc quyền trong hệ thống mục tiêu. - Ảnh hưởng: Windows 7/8.1/10/11, Windows Server 2022/2019/2016/2012/2008.	https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2022-26925
2	CVE-2022-26923	- Điểm CVSS: 8.8 (Cao) - Lỗ hổng trong Active Directory Domain Services cho phép đối tượng tấn công thực hiện nâng cao đặc quyền. - Ảnh hưởng: Windows 8.1/10/11, Windows Server 2012/2016/2019/2022.	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-24491
3	CVE-2022-26937	- 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 Server 2008/2012/2016/2019/2022.	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-26937
4	CVE-2022-29972	- Lỗ hổng trong Magnitude Simba Amazon Redshift ODBC Driver cho phép đối tượng thực thi mã từ xa.	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-29972 https://msrc-blog.microsoft.com/2022/05/09/vulnerability-mitigated-in-the-third-party-data-connector-used-in-azure-synapse-pipelines-and-azure-data-factory-cve-2022-29972
5	CVE-2022-21978	- Điểm CVSS: 8.2 (Cao) - Lỗ hổng trong Microsoft	https://msrc.microsoft.com/update-

		Exchange Server cho phép đối tượng tấn công thực hiện nâng cao đặc quyền. - Ảnh hưởng: Windows Server 2013/2016/2019.	guide/vulnerability/CVE-2022-21978
6	CVE-2022-22017	- Điểm CVSS: 8.8 (Cao) - Lỗ hổng trong Remote Desktop Protocol Client cho phép đối tượng tấn công thực thi mã từ xa. - Ảnh hưởng: Windows 11, Windows Server 2022.	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-22017
7	CVE-2022-29110	- Điểm CVSS: 7.8 (Cao) - Lỗ hổng trong Microsoft Excel cho phép đối tượng tấn công thực thi mã từ xa. - Ảnh hưởng: Microsoft Office Web Apps Server 2013, Microsoft Excel 2013/2016.	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-29110
8	CVE-2022-29108	- 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 SharePoint Server 2016/2019, Microsoft SharePoint Foundation 2013.	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-29108

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-May

https://www.zerodayinitiative.com/blog/2022/5/10/the-may-2022-security-update-review