UBND TỈNH TUYÊN QUANG
SỞ THÔNG TIN VÀ TRUYỀN THÔNG

CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM
Độc lập – Tự do – Hạnh Phúc

Số: 525 /STTTT-CNTT&BCVT
V/v lỗ hổng bảo mật ảnh hưởng cao và nghiêm trọng trong các sản phẩm Microsoft công bố tháng 5/2022

Tuyên Quang, ngày 18 tháng 5 năm 2022

Kính gửi:
- Văn phòng Đoàn Đại biểu Quốc hội và Hội đồng nhân dân tỉnh;
- Văn phòng Ủy ban nhân dân tỉnh;
- Các sở, ban, ngành;
- Uỷ ban nhân dân các huyện, thành phố;
- Trung tâm Công nghệ thông tin và Truyền thông, Sở Thông tin và Truyền thông.

Căn cứ văn bản số 674/CATTT – NCSC ngày 11/5/2022 của Cục An toàn thông tin về việc lỗ hổng bảo mật ảnh hưởng cao và nghiêm trọng trong các sản phẩm Microsoft công bố tháng 5/2022;

Sở Thông tin và Truyền thông cảnh báo tới các cơ quan, đơn vị, thông tin cụ thể như sau:

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

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).

II. Các giải pháp phòng tránh

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 không gian mạng Việt Nam, Sở Thông tin và Truyền thông đề nghị các sở, ban, ngành, Ủy ban nhân dân các huyện, thành phố triển khai thực hiện:

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 (tham khảo thông tin tại phụ lục kèm theo).

2. 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.

3.Trong trường hợp cần thiết có thể liên hệ đầu mối hỗ trợ của Cục An toàn thông tin: Trung tâm Giám sát an toàn không gian mạng quốc gia, điện thoại 02432091616, thư điện tử: ais@mic.gov.vn.

Trân trọng./.

Nơi nhận:
- Như trên;
- Ban Giám đốc sở (báo cáo);
- Lưu: VT, CNTT&BCVT

KT. GIÁM ĐỐC
PHÓ GIÁM ĐỐC

CỘNG HOÀ X.H.C.N VIỆT NAM
SỞ THÔNG TIN VÀ TRUYỀN THÔNG
TỈNH TUYÊN QUANG

Nguyễn Văn Hiến

Phụ lục

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

(Kèm theo Công văn số 525 /STTTT-CNTT&BCVT ngày 18 /5/2022 của Sở Thông tin và Truyền thông)

1.Thông tin các lỗ hổng bảo mật

STT	CVE	Mô tả	Link tham khảo
1	CVE-2022-26925	- 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, WindowsServer 2022/2019/2016/2012/2008	https://msrc.microsoft.com/updateguide/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, Server 2012/2016 /2019/2022.	https://msrc.microsoft.com/update-guide/vulnerability/CV E-2022-24491
3	CVE-2022-26937	- ĐiểmCVSS: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/CV E-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/CV E-2022-29972 https://msrc-blog.microsoft.com/20

			22/05/09/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 Exchange Server cho phép đối tượng tấn công thực hiện nâng cao đặc quyền. - Ảnh hưởng: Windows Server 2013/2016/2019.	https://msrc.microsoft. com/update-guide/vulnerability/CV E-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/CV E-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/CV E-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/CV E-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