UBND TỈNH TUYÊN QUANG
SỞ THÔNG TIN VÀ TRUYỀN THÔNG

Số:1194 /STTTT-CNTT&BCVT
V/v lỗ hổng bảo mật ảnh hưởng cao và nghiêm trọng trong các sản phẩm Microsoft công bố tháng 10/2022.

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

Tuyên Quang, ngày 18 tháng 10 năm 2022

Kính gửi:
- Văn phòng Đoàn Đại biểu Quốc hội và Hội đồng nhân dân;
- Văn phòng Ủy ban nhân dân tỉnh;
- Các sở, ban, ngành;
- Các tổ chức - Chính trị xã hội;
- Uỷ ban nhân dân các huyện, thành phố.

Căn cứ văn bản số 1559/CATTT-NCSC ngày 10/10/2022 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 10/2022, Sở Thông tin và Truyền thông cung cấp thông tin và đưa ra các giải pháp phòng, tránh khai thác lỗ hổng bảo mật trong các sản phẩm Microsoft như sau:

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

Ngày 11/10/2022, Microsoft đã phát hành danh sách bản vá tháng 10 với 85 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 có mức ảnh hưởng cao và nghiêm trọng sau:

- Lỗ hổng bảo mật **CVE-2022-41033** trong Windows COM + Event System Service cho phép đối tượng tấn công thực hiện nâng cao đặc quyền. Lỗ hổng này đã được một số nhóm tấn công khai thác trong thực tế.

- 02 lỗ hổng bảo mật **CVE-2022-37987, CVE-2022-37989** trong Windows Client Server Run-time Subsystem (CSRSS) cho phép đối tượng tấn công thực hiện nâng cao đặc quyền.

- Lỗ hổng bảo mật **CVE-2022-37968** trong Azure Arc-enabled Kubernetes cluster Connect cho phép đối tượng tấn công thực hiện nâng cao đặc quyền.

- 03 lỗ hổng bảo mật **CVE-2022-38048, CVE-2022-41043, CVE-2022-38001** trong Microsoft Office cho phép đối tượng tấn công thực thi mã từ xa, thu thập thông tin, tấn công giả mạo (Spoofing). Trong đó lỗ hổng **CVE-2022-41043** đã được công bố rộng rãi trên Internet.

- 03 lỗ hổng bảo mật **CVE-2022-41036, CVE-2022-41037, CVE-2022-**

41038 trong Microsoft SharePoint Server cho phép đối tượng tấn công thực thi mã từ xa.

- Lỗ hổng bảo mật **CVE-2022-41031** trong Microsoft Word cho phép đối tượng tấn công thực thi mã từ xa.

- Lỗ hổng bảo mật **CVE-2022-37976** trong Active Directory Certificate Services cho phép đối tượng tấn công thực hiện nâng cao đặc quyền.

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

2. Các giải pháp phòng tránh

Nhằm đảm bảo an toàn thông tin cho hệ thống thông tin của Quý đơn vị, góp phần bảo đảm an toàn cho không gian mạng Việt Nam, Sở Thông tin và Truyền thông khuyến nghị Quý đơn vị thực hiện:

1. Kiểm tra, rà soát, xác định thiết bị 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);
- Các đơn vị thuộc sở;
- 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 1194/STTTT-CNTT&BCVT ngày 18 /10 /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-2022-41033	- Điểm CVSS: 7.8 (Cao) - Lỗ hổng trong Windows COM + Event System Service cho phép đối tượng tấn công thực hiện nâng cao đặc quyền. Lỗ hổng này đã được một số nhóm tấn công khai thác trong thực tế. - Ảnh hưởng: Windows 7/8.1/10/11, Windows Server 2008/2012/2016/2019/2022.	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-41033
2	CVE-2022-37987 CVE-2022-37989	- Điểm CVSS: 7.8 (Cao) - Lỗ hổng trong trong Windows Client Server Run-time Subsystem (CSRSS) 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/vulnerability/CVE-2022-37987 https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-37989
3	CVE-2022-37968	- Điểm CVSS: 10 (Nghiêm trọng) - Lỗ hổng trong Azure Arc-enabled Kubernetes cluster Connect cho phép đối tượng tấn công thực hiện nâng cao đặc quyền. - Ảnh hưởng: Azure Stack Edge, Azure Arc-enabled Kubernetes cluster 1.6.19/1.5.8/1.7.18/1.8.11	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-37968
4	CVE-2022-38048	- Điểm CVSS: 7.8 (Cao)	https://msrc.microsoft.

Stt	CVE	Mô tả	Link tham khảo
	CVE-2022-41043 CVE-2022-38001	- Lỗ hổng trong trong Microsoft Office cho phép đối tượng tấn công thực thi mã từ xa, thu thập thông tin, tấn công giả mạo (Spoofing). - Ảnh hưởng: Microsoft Office 2013/2016/2019, Office 365 Apps, Office LTSC.	com/update-guide/vulnerability/CVE-2022-38048 https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-41043 https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-38001
5	CVE-2022-41036 CVE-2022-41037 CVE-2022-41038	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 2016/2019, SharePoint Foundation/Enterprise Server 2013.	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-41036 https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-41037 https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-41038
6	CVE-2022-41031	- Điểm CVSS: 7.8 (Cao) - Lỗ hổng trong Microsoft Word cho phép đối tượng tấn công thực thi mã từ xa. - Ảnh hưởng: Microsoft 365 Apps, Microsoft Office 2019/LTSC.	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-41031
7	CVE-2022-37976	Điểm CVSS: 8.8 (Cao) - Lỗ hổng trong Active Directory Certificate Services cho phép đối tượng tấn công thực hiện nâng cao đặc quyền. - Ảnh hưởng: Windows Server 2008/2012/2016/2019/ 2022	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-37976

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-Oct

https://www.zerodayinitiative.com/blog/2022/10/11/the-october-2022-security-update-review