UBND TỈNH TÂY NINH
SỞ THÔNG TIN VÀ TRUYỀN THÔNG

Số: 1577 /STTTT-TTGSĐH
V/v cảnh báo lỗ hổng bảo mật có mức ảnh hưởng Cao trong các sản phẩm Microsoft công bố tháng 10/2022

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

Tây Ninh, ngày17 tháng 10 năm 2022

Kính gửi:

- Văn phòng Tỉnh ủy;
- Văn phòng Đoàn ĐBQH và HĐND tỉnh;
- Văn phòng UBND tỉnh;
- Các cơ quan tham mưu, giúp việc Tỉnh ủy;
- Mặt trận Tổ quốc và các Đoàn thể chính trị - xã hội;
- Các Sở, ban, ngành tỉnh;
- Các huyện, thị, thành ủy trực thuộc Tỉnh ủy;
- UBND các huyện, thị xã, thành phố.

Thực hiện theo Công văn số 1559/CATTT-NCSC của Cục An toàn thông tin - Bộ Thông tin và Truyền thông về việc cảnh báo lỗ hổng bảo mật ảnh hưởng cao và nghiêm trọng trong các sản phẩm Microsoft công bố tháng 10/2022 ***(Thông tin chi tiết phụ lục kèm theo)***.

Nhằm đảm bảo an toàn thông tin cho hệ thống thông tin cho người dùng, đơn vị và toàn bộ hệ thống của tỉnh, Sở Thông tin và Truyền thông đề nghị các đơn vị, địa phương thực hiện gấp các công việc cụ thể như sau:

1. Kiểm tra, rà soát, xác định máy tính sử dụng hệ điều hành Windows và phần mềm có khả năng bị ảnh hưởng. Thực hiện cập nhật bản vá kịp thời theo hướng dẫn tại phụ lục để tránh nguy cơ bị tấn công.

2. Tăng cường kiểm tra, giám sát hệ thống mạng của đơn vị, địa phương, khi có phát hiện hoạt động tấn công mạng, đề nghị liên hệ Sở Thông tin và Truyền thông để phối hợp xử lý kịp thời.

Thông tin liên quan đề nghị liên hệ Ông Vương Duy Thanh - Trung tâm Giám sát, điều hành kinh tế, xã hội tập trung; Điện thoại: 0932624462.

Trân trọng./.

Nơi nhận:
- Như trên;
- GĐ Sở (b/c);
- P.CNTTBCVT;
- Lưu: VT, TTGSĐH.

KT. GIÁM ĐỐC
PHÓ GIÁM ĐỐC

CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM
SỞ THÔNG TIN VÀ TRUYỀN THÔNG
TỈNH TÂY NINH

Nguyễn Trung Hiếu

PHỤ LỤC
Thông tin các lỗ hổng nghiêm trọng trong các sản phẩm Microsoft công bố tháng 10/2022

1.Thông tin lỗ hổng bảo mật

- Mô tả:

- 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.

- Ảnh hưởng:

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

Stt	CVE	Mô tả	Link tham khảo
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 CVE-2022-41043 CVE-2022-38001	- Điểm CVSS: 7.8 (Cao) - 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.	https://msrc.microsoft.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	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-41036 https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-41037

Stt	CVE	Mô tả	Link tham khảo
		Foundation/Enterprise Server 2013.	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

- Đánh giá mức độ: Đánh giá sơ bộ từ các chuyên gia bảo mật, lỗ hổng này ảnh hưởng đến nhiều thiết bị trên toàn cầu trong đó có cả Việt Nam. Trung tâm Giám sát an toàn không gian mạng quốc gia (NCSC) đánh giá khả năng các mã khai thác của các lỗ hổng này sẽ sớm được công khai trên Internet trong thời gian sắp tới.

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. Nguồn 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