

Số: /STTTT-BCVT&CNTT

Quảng Ngãi, ngày 14 tháng 10 năm 2022

V/v cảnh báo lỗ hổng bảo mật ảnh hưởng cao trong các sản phẩm Microsoft công bố tháng 10/2022

Kính gửi:

- Văn phòng: Tỉnh ủy, Đoàn ĐBQH&HĐND, UBND tỉnh;
- Các sở, ban, ngành; Hội, đoàn thể tỉnh;
- UBND các huyện, thị xã, thành phố;
- Báo Quảng Ngãi, Đài Phát thanh và Truyền hình tỉnh;
- Phòng An ninh mạng và phòng, chống tội phạm sử dụng công nghệ cao - Công an tỉnh;
- UBND các xã, phường, thị trấn.

Theo cảnh báo của Cục An toàn thông tin tại Công văn số 1559/CATTT-NCSC ngày 23/9/2022 về 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 đề nghị lãnh đạo các cơ quan, đơn vị chỉ đạo thực hiện một số biện pháp sau để hạn chế các rủi ro về nguy cơ mất an toàn thông tin:

1. Kiểm tra, rà soát máy chủ, máy trạm có sử dụng hệ điều hành Windows để phát hiện và xử lý kịp thời các máy chủ có khả năng bị ảnh hưởng bởi các lỗ hổng bảo mật 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.

(Tham khảo thông tin lỗ hổng và cách khắc phục tại Phụ lục Thông tin về lỗ hổng bảo mật kèm theo Công văn này)

2. Khi phát hiện các hệ thống có biểu hiện bị khai thác, tấn công mạng, triển khai ngay các biện pháp xử lý ngăn chặn tấn công trên hệ thống và thông báo về Đội ứng cứu sự cố an toàn thông tin mạng tỉnh Quảng Ngãi để có các biện pháp hỗ trợ, xử lý kịp thời.

Đề nghị lãnh đạo các cơ quan, đơn vị quan tâm chỉ đạo thực hiện./.

Nơi nhận:

- Như trên;
- Cục An toàn thông tin (báo cáo);
- Phòng VH&TT các huyện, thị xã, thành phố;
- Thành viên Đội ứng cứu sự cố ATTT mạng tỉnh;
- Sở TT&TT: Lãnh đạo Sở, các phòng chuyên môn, TT CNTT&TT;
- Lưu: VT, BCVT&CNTT.

**KT. GIÁM ĐỐC
PHÓ GIÁM ĐỐC**

Đỗ Quang Nghĩa

PHỤ LỤC
THÔNG TIN VỀ CÁC LỖ HỔNG BẢO MẬT TRONG MICROSOFT
*(Kèm theo Công văn số /STTTT-BCVT&CNTT ngày /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	<ul style="list-style-type: none"> - 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	<ul style="list-style-type: none"> - Điểm CVSS: 7.8 (Cao) - Lỗ hổng trong Windows Client Server Runtime 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	<ul style="list-style-type: none"> - 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	<ul style="list-style-type: none"> - Điểm CVSS: 7.8 (Cao) - Lỗ hổng trong Microsoft Office cho phép 	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-38048

Stt	CVE	Mô tả	Link tham khảo
		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.	E-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>