UBND TỈNH QUẢNG NGÃI
SỞ THÔNG TIN VÀ TRUYỀN THÔNG

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

Số:1873 /STTTT-BCVT&CNTT

Quảng Ngãi, ngày 15 tháng 12 năm 2022

V/v cảnh báo lỗ hổng bảo mật ảnh hưởng cao trong các sản phẩm Microsoft công bố tháng 12/2022

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 2035/CATTT-NCSC ngày 14/12/2022 về lỗ hổng bảo mật ảnh hưởng Cao và Nghiêm trọng trong các sản phẩm Microsoft công bố tháng 12/2022; 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-2022-44698** trong Windows SmartScreen cho phép đối tượng tấn công thực hiện tấn công vượt qua cơ chế bảo mật. Lỗ hổng này đang bị khai thác trong thực tế.

- Lỗ hổng bảo mật **CVE-2022-41076** trong PowerShell cho phép đối tượng tấn công thực thi mã từ xa. Lỗ hổng này ảnh hưởng đến nhiều sản phẩm như: Microsoft Exchange Server, Skype for Business Server,…

- Lỗ hổng bảo mật **CVE-2022-44713** trong Microsoft Outlook for Mac cho phép đối tượng tấn công thực hiện tấn công giả mạo (spoofing).

- Lỗ hổng bảo mật **CVE-2022-44699** trong Azure Network Watcher Agent cho phép đối tượng tấn công thực hiện tấn công vượt qua cơ chế bảo mật.

- Lỗ hổng **CVE-2022-44710** trong DirectX Graphics Kernel cho phép đối tượng tấn công thực hiện nâng cao đặc quyền. Lỗ hổng này đã có mã khai thác được công bố rộng rãi trên Internet.

- 02 lỗ hổng bảo mật **CVE-2022-44690, CVE-2022-44693** trong Microsoft SharePoint Server cho phép đối tượng tấn công thực thi mã từ xa.

- 02 lỗ hổng bảo mật **CVE-2022-44678, CVE-2022-44681** trong Windows

Print Spooler cho phép đối tượng tấn công thực hiện nâng cao đặc quyền.

- 02 lỗ hổng bảo mật **CVE-2022-44708, CVE-2022-41115** trong Microsoft Edge (Chromium-based) cho phép đối tượng tấn công thực hiện nâng cao đặc quyền.

- Lỗ hổng bảo mật **CVE-2022-44673** trong Windows Client Server Run-Time Subsystem (CSRSS) 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

CỘNG HÒA X.H.C.N VIỆT NAM
SỞ THÔNG TIN VÀ TRUYỀN THÔNG
TỈNH QUẢNG NGÃI

Đỗ Quang Nghĩa

PHỤ LỤC
THÔNG TIN VỀ CÁC LỖ HỔNG BẢO MẬT TRONG MICROSOFT

(Kèm theo Công văn số /STTTT-BCVT&CNTT ngày 15/12/2022 của Sở Thông tin và Truyền thông)

1. Thông tin các lỗ hổng bảo mật

STT	CVE	Mô tả	Link tham khảo
1	CVE-2022-44698	- Điểm: CVSS: 5.4 - Mô tả: lỗ hổng trong Windows SmartScreen cho phép đối tượng tấn công thực hiện tấn công vượt qua cơ chế bảo mật. Lỗ hổng này đang bị khai thác trong thực tế. - Ảnh hưởng: Windows 10/11, Windows Server 2016/2019/2022.	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-44698
2	CVE-2022-41076	- Điểm CVSS: 8.5 (Cao) - Mô tả: lỗ hổng trong PowerShell cho phép đối tượng tấn công thực thi mã từ xa. - Ảnh hưởng: Windows 7/8.1/10/11, Windows Server 2008/2012/2016/2019/2022, PowerShell 7.2/7.3.	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-41076
3	CVE-2022-44713	- Điểm CVSS: 7.5 (Cao) - Mô tả: lỗ hổng trong Microsoft Outlook for Mac cho phép đối tượng tấn công thực hiện tấn công giả mạo (spoofing). - Ảnh hưởng: Microsoft Office 2019 for Mac, Office LTSC for Mac 2021.	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-44713
4	CVE-2022-44699	- Điểm CVSS: 5.5 - Mô tả: lỗ hổng trong Azure Network Watcher Agent cho phép đối tượng tấn công thực hiện tấn công vượt qua cơ chế bảo mật.	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-44699

STT	CVE	Mô tả	Link tham khảo
		- Ảnh hưởng: Azure Network Watcher Vm Extension.	
5	CVE-2022-44710	- Điểm CVSS: 7.8 (Cao) - Mô tả: lỗ hổng trong DirectX Graphics Kernel cho phép đối tượng tấn công thực hiện nâng cao đặc quyền. Lỗ hổng này đã có mã khai thác được công bố rộng rãi trên Internet. - Ảnh hưởng: Windows 11.	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-44710
6	CVE-2022-44678, CVE-2022-44681	- Điểm CVSS: 8.8 (Cao) - Mô tả: lỗ hổng trong Windows Print Spooler 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.	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-44678 https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-44681
7	CVE-2022-44690, CVE-2022-44693	- Điểm CVSS: 8.8 (Cao) - Mô tả: trong Microsoft SharePoint Server cho phép đối tượng tấn công thực thi mã từ xa. - Ảnh hưởng: Microsoft SharePoint Server 2019, SharePoint Foundation 2013, SharePoint Enterprise Server 2013/2016.	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-44690 https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-44693
8	CVE-2022-44708, CVE-2022-41115	- Điểm CVSS: 8.3 (Cao) - Mô tả: Lỗ hổng trong Microsoft Edge (Chromium-based) cho phép đối tượng tấn công thực hiện nâng cao đặc quyền. - Ảnh hưởng: Microsoft Edge	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-44708 https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-41115

STT	CVE	Mô tả	Link tham khảo
9	CVE-2022-44673	- Điểm CVSS: 7.0 (Cao) - Mô tả: Lỗ hổng 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, Windows Server 2008.	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-44673

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/en-us

https://www.zerodayinitiative.com/blog/2022/12/13/the-december-2022-security-update-review