UBND TỈNH QUẢNG NGÃI
SỞ GIÁO DỤC VÀ ĐÀO TẠO

Số: 524 /TB-SGDĐT

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

Quảng Ngãi, ngày 16 tháng 5 năm 2022

THÔNG BÁO
Cảnh báo lỗ hổng bảo mật ảnh hưởng Cao và Nghiêm trọng trong các sản phẩm Microsoft công bố tháng 5/2022

Theo đề nghị của Sở Thông tin và Truyền thông tại Công văn số 624/STTTT-BCVT&CNTT ngày 13/5/2022 về việc cảnh báo lỗ hổng bảo mật ảnh hưởng Cao và Nghiêm trọng trong các sản phẩm Microsoft công bố tháng 5/2022;

Sở Giáo dục và Đào tạo thông báo đến các đơn vị, cơ sở giáo dục kiểm tra, rà soát để phát hiện và xử lý kịp thời các hệ thống thông tin có khả năng bị ảnh hưởng bởi lỗ hổng bảo mật trong các sản phẩm Microsoft công bố tháng 5/2022. *(Kèm theo Công văn số 624/STTTT-BCVT&CNTT ngày 13/5/2022 của Sở Thông tin và Truyền thông).*

Yêu cầu lãnh đạo các đơn vị quan tâm chỉ đạo thực hiện./.

***Nơi nhận*:**
- Đơn vị trực thuộc Sở GDĐT;
- Phòng GDĐT huyện, thị xã, thành phố;
- Trung tâm GDNN-GDTX huyện, thị xã;
- Lãnh đạo Sở GDĐT;
- Các phòng thuộc Sở GDĐT;
- Lưu: VT, VP, ndh.

TL. GIÁM ĐỐC
KT. CHÁNH VĂN PHÒNG
PHÓ CHÁNH VĂN PHÒNG

CỘNG HÒA X.H.C.N VIỆT NAM
SỞ GIÁO DỤC VÀ ĐÀO TẠO
TỈNH QUẢNG NGÃI

Nguyễn Đức Huân

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:624 /STTTT-BCVT&CNTT	*Quảng Ngãi, ngày 13 tháng 5 năm 2022*

V/v cảnh báo lỗ hổng bảo mật ảnh hưởng Cao và Nghiêm trọng trong các sản phẩm Microsoft công bố tháng 5/2022

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.

Theo cảnh báo của Cục An toàn thông tin tại Công văn số 674/CATTT-NCSC ngày 11/5/2022 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 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-2022-26925** 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.

- 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.

Đây là các lỗ hổng nguy hiểm *(có mức ảnh hưởng Nghiêm trọng và Cao)*, cần thực hiện cập nhật bản vá kịp thời để tránh nguy cơ bị tấn công đối với các thiết bị bị ảnh hưởng theo hướng dẫn của Microsoft *(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;
- 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 /5/2022 của Sở Thông tin và Truyền thông)

1. Thông tin các lỗ hổng bảo mật

TT	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 relayattack từ đó nâng cao đặc quyền trong hệ thống mục tiêu. - Ảnh hưởng: Windows 7/8.1/10/11, Windows Server 2022/2019/2016/2012/2008.	https://msrc.microsoft.com/update-guide/enUS/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, Windows Server 2012/2016/2019/2022.	https://msrc.microsoft.com/updateguide/vulnerability/CVE-2022-4491
3	CVE-2022-26937	- Điểm CVSS: 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/updateguide/vulnerability CVE-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/updateguide/vulnerability/CV-2022-29972 https://msrcblog.icrosoft.com/2022/05/09/vulnerabilitmitigated-in-the-thirdparty-data-connectorused-in-azure-synapsepipelines-and-azuredata-

TT	CVE	Mô tả	Link tham khảo
			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/updateguide/vulnerability/CVE-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/updateguide/vulnerability/CVE-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: MicrosoftOffice Web Apps Server 2013, Microsoft Excel 2013/2016.	https://msrc.microsoft.com/updateguide/vulnerability/CVE-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/updateguide/vulnerability/CVE-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