UBND TỈNH QUẢNG NGÃI **SỞ GIAO THÔNG VẬN TẢI**	**CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM** **Độc lập - Tự do - Hạnh phúc**
Số: 1524 /SGTVT-VP V/v cảnh báo lỗ hổng bảo mật ảnh hưởng cao trong các sản phẩm Microsoft công bố tháng 6/2022	*Quảng Ngãi, ngày 22 tháng 6 năm 2022*

Kính gửi:
- Các phòng chuyên môn, nghiệp vụ Sở;
- Các đơn vị trực thuộc Sở.

Sở Giao thông vận tải nhận được Công văn số 823/STTTT-BCVT&CNTT ngày 17/6/2022 của Sở Thông tin và Truyền thông về việc cảnh báo lỗ hổng bảo mật ảnh hưởng cao trong các sản phẩm Microsoft công bố tháng 6/2022; Để thực hiện các biện pháp nhằm hạn chế các rủi ro về nguy cơ mất an toàn thông tin, Giám đốc Sở yêu cầu Trưởng các phòng chuyên môn, nghiệp vụ Sở, Thủ trưởng các đơn vị trực thuộc Sở triển khai một số công việc sau:

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, máy trạm có khả năng bị ảnh hưởng bởi các lỗ hổng bảo mật sau:

- Lỗ hổng bảo mật **CVE-2022-30190** *(hay còn gọi là Follina)* trong Windows Microsoft Support Diagnotic Tool (MSDT) cho phép đối tượng tấn công thực thi mã tùy ý *(thực hiện theo hướng dẫn tại Công văn số 1293/SGTVT-VP ngày 06/6/2022 của Sở Giao thông vận tải về việc cảnh báo lỗ hổng bảo mật CVE-2022-30190 trong Microsoft Support Diagnostic Tool để vá lỗi)*.

- Lỗ hổng bảo mật **CVE-2022-30136** trong Windows Network File System cho phép đối tượng tấn công không cần xác thực có thể thực thi mã từ xa.

- Lỗ hổng bảo mật **CVE-2022-30163** trong Windows Hyper-V cho phép đối tượng tấn công thực thi mã từ xa.

- Lỗ hổng bảo mật **CVE-2022-30139** trong Windows Lightweight Directory Access Protocol (LDAP) cho phép đối tượng tấn công thực thi mã từ xa.

- 02 lỗ hổng bảo mật **CVE-2022-30157, CVE-2022-30158** trong Microsoft SharePoint Server cho phép đối tượng tấn công thực thi mã từ xa.

- Lỗ hổng bảo mật **CVE-2022-30165** trong Windows Kerberos cho phép đối tượng tấn công thực hiện tấn công nâng cao đặc quyền.

- Lỗ hổng bảo mật **CVE-2022-30173** Microsoft Excel cho phép đối tượng tấn công thực thi mã từ xa.

- Lỗ hổng bảo mật **CVE-2022-30174** trong Microsoft Office cho phép đối tượng tấn công thực thi mã từ xa.

Đây là các lỗ hổng bảo mật ảnh hưởng 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 *(thông tin lỗ hổng và cách khắc phục tại Phụ lục Thông tin về lỗ hổng bảo mật trong Microsoft gửi kèm theo Công văn này)*.

2. Tăng cường kiểm tra, giám sát và sẵn sàng phương án xử lý khi phát hiện có dấu hiệu bị khai thác, tấn công mạng; 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 Sở Giao thông vận tải *(qua Văn phòng Sở)* để có các biện pháp hỗ trợ, xử lý kịp thời.

Giám đốc Sở yêu cầu Trưởng các phòng chuyên môn, nghiệp vụ Sở, Thủ trưởng các đơn vị trực thuộc Sở triển khai thực hiện nghiêm túc./.

Nơi nhận:
- Như trên;
- Sở TT&TT;
- Lãnh đạo Sở;
- Lưu: VT, VP(Dũng).

GIÁM ĐỐC

CỘNG HÒA X.H.C.N. VIỆT NAM
SỞ GIAO THÔNG VẬN TẢI
TỈNH QUẢNG NGÃI

Nguyễn Phong

Phụ lục

THÔNG TIN VỀ CÁC LỖ HỔNG BẢO MẬT TRONG MICROSOFT

(Kèm theo Công văn số /SGTVT-VP ngày /6/2022 của Sở GTVT)

1. Thông tin các lỗ hổng bảo mật

STT	CVE	Mô tả	Link tham khảo
1	CVE-2022-30190 (Follina)	- Điểm CVSS: 7.8 (Cao) - Lỗ hổng trong Windows Microsoft Support Diagnotic Tool (MSDT) cho phép đối tượng tấn công thực thi mã tùy ý. - Ảnh hưởng: Windows 7/8.1/10, Windows Server 2008/2012/2016.	https://msrc.microsoft.com/update-guide/enUS/vulnerability/CVE-2022-30190
2	CVE-2022-30136	- Điểm CVSS: 9.8 (Nghiêm trọng) - Lỗ trong Windows Network File System cho phép đối tượng tấn công không cần xác thực có thể thực thi mã từ xa. - Ảnh hưởng: Windows Server 2012/2016/2019.	https://msrc.microsoft.com/updateguide/vulnerability/CVE-2022-30136
3	CVE-2022-30163	- Điểm CVSS: 8.5 (Cao) - Lỗ hổng trong Windows Hyper-V cho phép đối tượng tấn công thực thi mã từ xa. - Ảnh hưởng: Windows 8.1/10/11, Windows Server 2008/2012/2016.	https://msrc.microsoft.com/updateguide/vulnerability/CVE-2022-30163
4	CVE-2022-30139	- Điểm CVSS:7.5 (cao) - Lỗ hổng trong Windows Lightweight Directory Access Protocol (LDAP) cho phép đối tượng tấn công thực thi mã từ xa. - Ảnh hưởng: Windows 10, Windows Server 2016/2019/2022.	https://msrc.microsoft.com/updateguide/vulnerability/CVE-2022-30139
5	CVE-2022-	- Điểm CVSS: 8.8 (Cao)	https://msrc.microsoft.co

STT	CVE	Mô tả	Link tham khảo
	30157 CVE-2022-30158	- Lỗ hông trong Microsoft SharePoint Server cho phép đối tượng tấn công thực thi mã từ xa. - Ảnh hưởng: SharePoint Server 2019, SharePoint Enterprise Server 2016.	m/updateguide/vulnerability/CVE-2022-30157https://msrc.microsoft.com/updateguide/vulnerability/CVE-2022-30158
6	CVE-2022-30165	- Điểm CVSS: 8.8 (Cao) - Lỗ hổng trong Windows Kerberos cho phép đối tượng tấn công thực hiện tấn công nâng cao đặc quyền. - Ảnh hưởng: Windows 10/11, Windows Server 2016/2022.	https://msrc.microsoft.com/updateguide/vulnerability/CVE-2022-30165
7	CVE-2022-30173	- Điểm CVSS: 7.8 (Cao) - Lỗ hổng trong Microsoft Excel cho phép đối tượng tấn công thực thi mã từ xa. - Ảnh hưởng: Excel 2013/2016.	https://msrc.microsoft.com/updateguide/vulnerability/CVE-2022-30173
8	CVE-2022-30174	- Điểm CVSS: 7.4 (Cao) - Lỗ hổng trong Microsoft Office cho phép đối tượng tấn công thực thi mã từ xa. - Ảnh hưởng: Microsoft 365 Apps, Microsoft Office LTSC 2021.	https://msrc.microsoft.com/updateguide/vulnerability/CVE-2022-30174

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-Jun

https://www.zerodayinitiative.com/blog/2022/6/14/the-june-2022-security-update-review